UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA MECÂNICA

ANÁLISE DA SISTEMÁTICA DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS CIBERNÉTICOS: ESTUDO DE CASO COMPARATIVO ENTRE EMPRESAS E ÓRGÃOS REGULADORES

RHOXANNA CRHISTIANTH FARAGO MIRANDA

ORIENTADOR: SANDERSON CÉSAR MACÊDO BARBALHO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA MECATRÔNICA

BRASÍLIA
2017

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA MECÂNICA

ANÁLISE DA SISTEMÁTICA DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS CIBERNÉTICOS: ESTUDO DE CASO COMPARATIVO ENTRE EMPRESAS E ÓRGÃOS REGULADORES

RHOXANNA CRHISTIANTH FARAGO MIRANDA

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA MECÂNICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA MECATRÔNICA.

APROVADO POR:

_____

Prof. Dr. Sanderson César Macêdo Barbalho (ORIENTADOR)

_____

Prof. Dr. Paulo Roberto de Lira Gondim (EXAMINADOR INTERNO)

_____

Prof. Dr. Sérgio Luis da Silva (EXAMINADOR EXTERNO)

BRASÍLIA, 09 DE FEVEREIRO, 2017

FICHA CATALOGRÁFICA

M672

Miranda, Rhoxanna Christianth Farago

Análise da sistemática de homologação e certificação de produtos cibernéticos: estudo de caso comparativo entre empresas e órgãos reguladores / Rhoxanna Christianth Farago Miranda; orientador Sanderson César Macêdo Barbalho. -- Brasília, 2017.

155 f.

Dissertação (Mestrado - Mestrado em Engenharia Mecatrônica) -- Universidade de Brasília, 2017.

1. Cibernética. 2. Homologação. 3. Certificação. I. Barbalho, Sanderson César Macêdo, orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

MIRANDA, Rhoxanna Christianth Farago. **Análise da sistemática de homologação e certificação de produtos cibernéticos:** estudo de caso comparativo entre empresas e órgãos reguladores. 2017. 155 f. Dissertação (Mestrado) - Curso de Engenharia Mecatrônica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2017.

CESSÃO DE DIREITOS

AUTOR: Rhoxanna Christianth Farago Miranda

TÍTULO: Análise da sistemática de homologação e certificação de produtos cibernéticos: estudo de caso comparativo entre empresas e órgãos reguladores

GRAU: Mestre Ano: 2017

_____

Rhoxanna Crhistianth Farago Miranda
rhoxanna@gmail.com

AGRADECIMENTOS

À Deus, pela grandiosa força e luz na caminhada da vida, permitindo renovar as minhas forças a cada manhã.

Ao meu orientador Prof. Dr. Sanderson César Macêdo Barbalho, pelo aprendizado, orientações, sabedoria e confiança. Por me conceder a oportunidade de desenvolver um estudo alinhado ao projeto de apoio ao Programa de Defesa Cibernética. Por me convidar a participar do Projeto de Homologação e Certificação de Produtos Cibernéticos utilizados na Defesa Nacional.

Ao Prof. Dr. Edson Paulo da Silva, pela motivação e direcionamento acadêmico.

Ao Prof. Dr. Carlos Humberto Llanos, professor do 1° semestre na graduação do curso de Engenharia da Computação na disciplina Algoritmos e Programação de Computadores (APC) e também na disciplina Instrumentação, no mestrado.

À minha mãe Olga, pela força e otimismo pela vida e na realização dos sonhos.

Aos amigos que conheci ao longo dessa caminhada e que compartilharam suas experiências, levando os momentos difíceis com alegria e bom humor.

Ao meu pai (in memoriam) Francisco Miranda, pelo grande ensinamento à vida.

RESUMO

Esta dissertação realiza um diagnóstico da sistemática de homologação e certificação de produtos cibernéticos através da comparação com o Modelo de Referência Mecatrônico (MRM), para o desenvolvimento de produtos mecatrônicos, proposto por Barbalho (2006). Discute o conceito de produto cibernético como produto mecatrônico, destacando a existência desses produtos em infraestruturas de Tecnologias de Informação e Comunicação (TIC), assim como a necessidade de proteger tais produtos de ataques cibernéticos. Descreve os processos das fases de homologação (9) e validação (10) do MRM, assim como os documentos gerados ao final de cada uma. Fases estas, que serão utilizadas na elaboração dos formulários para realização do diagnóstico do estudo de caso em 5 empresas incluindo tanto o setor público como o privado. Utiliza dois formulários para a realização do diagnóstico: Formulário de Análise do Processo de Homologação do Produto e Formulário de Análise do Processo de Certificação do Produto, os quais são baseados em pergunta(s)/resposta(s). Apresenta-se um terceiro Fomulário de Análise baseado nos requisitos de segurança do produto descritos na Norma ISO/IEC_15408: *Common Criteria for Information Technology Security Evaluation* (2012), abordando as seguintes áreas: Perfil de Proteção, Desenvolvimento do produto, Documentação, Ciclo de Vida, Avaliação da Segurança, Testes, Análise de Vulnerabilidades e Níveis de garantia para avaliação do produto. O trabalho utiliza dois procedimentos de pesquisa: a pesquisa bibliográfica e o estudo de caso. A utilização do diagnóstico serviu para identificar as práticas de homologação e certificação empregadas pelas empresas e órgãos públicos do estudo de caso, sendo a base para sugerir melhorias para as empresas analisadas e diretrizes para órgãos públicos realizarem a aquisição de tais produtos. Verificou-se que o MRM, com algumas adaptações, incluindo requisitos previstos nas Normas ISO/IEC_15408 e IEEE 1012, pode ser aplicado para a homologação e certificação de produtos cibernéticos. Dessa forma, isso contribui na elaboração de estratégias de certificação e homologação de produtos cibernéticos. Além disso, permitiu identificar as lacunas na bibliografia pesquisada, como a inexistência de uma padronização para homologar e certificar produtos cibernéticos. Como direções para pesquisas futuras, sugere-se a exploração dos tipos de testes realizados pelos laboratórios acreditados, o que requer uma análise mais profunda e específica.

Palavras-chave: Cibernética. Homologação. Certificação. MRM. ISO/IEC-15408.

ABSTRACT

This dissertation performs diagnosis of the systematic of approval and cyber products certification through comparison with the Mechatronics Reference Model (MRM), for the development of mechatronic products, proposed by Barbalho (2006). Discusses the concept of cyber product as mechatronic product, highlighting the existence of these products in infrastructure of information and communication technologies (ICTs), as well as the need to protect such products from cyber-attacks. Describes the processes of phases of approval (9) and (10) MRM validation, as well as the documents generated at the end of each one. These phases will be used in the preparation of forms for diagnosis of the case study in 5 companies including both the public as the private sector. Are used two forms for the diagnosis: Form of analysis of the product approval process and Form of Analysis of the product Certification process, which are based on question(s) / answer(s). It is presented a third Form of analysis based on the security requirements of the product described in ISO/IEC_15408: *Common Criteria for Information Technology Security Evaluation* (2012), addressing the following areas: Profile, Product Development, Documentation, Lifecycle, Security assessment, Tests, Vulnerability analysis and Assurance levels for product evaluation. The work uses two research procedures: the bibliographical research and case study. The use of the diagnosis has served to identify the approval and certification practices employed by companies and public sectors in the case study, being the base to suggest improvements for companies reviewed and guidelines for public agencies to carry out the purchase of such products. It was found that the MRM, with some adaptations, including foreseen requirements in ISO/IEC_15408 and IEEE 1012 Standards, can be applied for the approval and certification of cyber products. Thereby, it contributes in the development of strategies for certification and approval of cyber products. Besides, it allows to identify the gaps in the researched bibliography, As the absence of standardization to homologate and certify products. As directions for future research, it is suggested the exploration of the types of tests performed by accredited laboratories, which requires a deeper and specific analysis.

Keywords: Cyber. Approval. Certification. MRM. ISO/IEC_15408.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ABS	*Anti-Lock Braking System*
AMR	*Advanced Manufacturing Research*
ANAC	Agência Nacional de Aviação Civil
ANATEL	Agência Nacional de Telecomunicações
APF	Administração Pública Federal
API	*Application Programming Interface*
APN	*Access Point Name*
ATA	Adaptador Telefônico Analógico
CAD	*Computer Aided Design*
CAE	*Computer Aided Engineering*
CAM	*Computer Aided Manufacturing*
CAN	*Controller Area Network*
CAPP	*Computer Aided Process Planning*
CC	*Common Criteria*
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos para Resposta e Tratamento de Incidentes para a Internet Brasileira.
CESVI Brasil	Centro de Experimentação e Segurança Viária
CGI	Comitê Gestor de Internet no Brasil
CLP	Controlador Lógico Programável
CPD	Centro de Processamento de Dados
CPS	*Cyber-Physical System*
CPU	*Central Processing Unit*
CSIRT	*Computer Security and Incident Response Team*
CTI	Centro de Tecnologia da Informação
DATAPREV	Empresa de Tecnologia e Informações da Previdência Social
DECEA	Departamento de Controle do Espaço Aéreo
DENATRAN	Departamento Nacional de Trânsito
DFMEA	*Design for manufacture and assembly*
DMZ	*DeMilitarized Zone*

DVD	*Digital Video Disc*
EAL	*Evaluation Assurance Level*
EAP	Estrutura Analítica do Projeto
ESC	*Electronic Stability Control*
FIPS	*Federal Information Processing Standard*
FMEA	*Failure Mode and Effect Analysis*
FMECA	*Failure Mode, Effect and Criticality Analysis*
FTP	*File Transfer Protocol*
GPRS	*General Packet Radio Services*
GPS	*Global Positioning System*
HD	*Hard Disk*
ICP Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection Systems*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electric and Electronic Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPS	*Intrusion Prevention Systems*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
LCD	*Liquid Crystal Display*
MCTI	Ministério da Ciência, Tecnologia e Inovação
MES	*Manufacturing Execution Systems*
MIT	*Massachusetts Institute of Technology*
MRM	Modelo de Referência Mecatrônico
NISC	*National Center of Incident Readiness and Strategy for Cybersecurity*
NIST	*National Institute of Standards and Technology*
NSC	Nível de Segurança de Certificação
OCP	Organismo de Certificação de Produto
PACs	Controladores Programáveis para Automação
PCIDSS	*Payment Card Industry Data Security Standard*
PDP	Processo de Desenvolvimento do Produto
PMBOK	*Project Management Body of Knowledge*

PoE	Power Over Ethernet
RoHS	*Restriction to the use of Hazardous Substances*
RFC	*Request for Comments*
PRODE	Produto Estratégico de Defesa
PP	*Protection Profile*
RGCP	Requisitos Gerais de Certificação de Produto
SAR	*Security Assurance Requirements*
SBAC	Sistema Brasileiro de Avaliação da Conformidade
SEPIN	Secretaria de Política de Informática
SERPRO	Serviço Federal de Processamento de Dados
SFR	*Security Functional Requirements*
SDCD	Sistema Digital de Controle Distribuído
SGCH	Sistema de Gestão de Certificação e Homologação
SGSI	Sistema de Gestão de Segurança da Informação
SOBRACON	Sociedade Brasileira de Comando Numérico
ST	*Security Target*
TAP	Termo de Abertura do Projeto
TCS	*Traction Control*
TCU	*Telematic Control Unit*
TELEBRAS	Telecomunicações Brasileiras S.A.
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicação
TSF	TOE *Security Functionality*
TSFI	TSF *Interface*
ToE	*Target of Evaluation*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

A cibernética se encontra inserida no mundo moderno, tecnológico, presente no cotidiano da vida das pessoas e das organizações, seja através das aplicações em um ambiente de rede corporativa ou na utilização de dispositivos tecnológicos como *notebooks*, *smartphones*, *tablets*, celulares, GPS, etc. Esses produtos apresentam características de integração de diversas tecnologias de controle e projetos de engenharia inteligente e se tornaram essenciais para a otimização das atividades organizacionais, o que os tornam também, vulneráveis a ataques cibernéticos. Como as organizações poderiam prover segurança para produtos tão complexos ? Como minimizar os ataques cibernéticos ? Como proteger infraestruturas críticas de Estado ? Como as empresas poderiam melhorar o processo de desenvolvimento de produtos (PDP) para disponibilizar no mercado produtos mais confiáveis e resistentes à evolução tecnológica relacionada aos ataques cibernéticos ?

O presente trabalho se encontra alinhado ao Modelo de Referência Mecatrônico (MRM), um modelo analítico para dar suporte ao desenvolvimento de produtos mecatrônicos, proposto por Barbalho (2006). A proposta é a realização do diagnóstico da sistemática de homologação e certificação de produtos cibernéticos utilizados pelas empresas do estudo de caso através da comparação com o MRM desenvolvido por Barbalho (2006). Apresenta-se a visão dos processos das fases de homologação e validação do MRM, assim como o detalhamento dos requisitos de segurança do produto propostos pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). O modelo analítico construído será utilizado para realizar estudos de caso em cinco empresas públicas e privadas no âmbito da cidade de Brasília, sendo a base para sugerir melhorias para as empresas analisadas e diretrizes para órgãos públicos.

1.1 CONTEXTUALIZAÇÃO E PROBLEMATIZAÇÃO DO TRABALHO

As empresas, independentemente da área de atuação, seja de base tecnológica, de energia elétrica, telecomunicações, sistema financeiro, órgãos do governo, dependem extremamente de tecnologias de informação e comunicação (TIC) na realização de suas atividades. Essa dependência de tecnologia, muitas vezes de origem estrangeira, tanto em relação aos produtos quanto aos serviços utilizados, engloba também normas e doutrinas de utilização, operação e manutenção desses produtos.

Esses produtos apresentam grande influência tanto no aspecto de privacidade como de forma mais macro, do controle do Estado sobre as ações de empresas e indivíduos, o que leva

o Brasil a aceitar uma legislação que impõe a disponibilização das informações produzidas por essas tecnologias para o uso do Governo, em aspectos de segurança e combate ao terrorismo (BARBALHO, 2006.). Essa problemática enfrentada pelo Brasil acontece também com outras potências, como a União Europeia que busca uma regulamentação do uso desses sistemas e tecnologias estrangeiras.

A evolução tecnológica caracterizada pelo alto grau de conectividade deu origem a outros tipos de problemas intrínsecos às novas tecnologias, como o aparecimento de novas vulnerabilidades. Muitos produtos lançados no mercado antes da concorrência já apresentam falhas. Por outro lado, diversos fatores contribuem com o aumento das vulnerabilidades, como a pressa no lançamento de um produto, nível de competitividade, crescente número de atacantes, integração de diversas tecnologias, complexidade do ambiente, dentre outros (NAKAMURA; GEUS, 2007). Neste contexto, todos esses produtos e o ambiente no qual atuam estão sujeitos a ataques cibernéticos dos mais diversos.

Pesquisas recentes publicadas em 2016 e realizadas pela empresa HP revelaram 2015 como o ano do chamado “dano colateral”, gerando vários impactos nas organizações, como roubo de dados de clientes, vazamento de cadastro, constatando prejuízos financeiros em torno de U$$ 400 bilhões de dólares ao ano, com ataques cibernéticos no mundo (OLIVEIRA, 2016). A definição de controles de segurança para defesa cibernética e os investimentos em segurança nas organizações devem ser vistos pela alta direção como um fator de relevância, podendo garantir o futuro da mesma perante o mercado.

Faz-se necessário o aperfeiçoamento dos produtos cibernéticos e o estabelecimento de critérios de segurança que reduzam as vulnerabilidades inerentes a um ambiente de TIC, no qual as empresas brasileiras se encontram inseridas. Alguns autores como Shafqat e Massod (2016) relatam a ausência de uma padronização em segurança cibernética em vários países de diferentes regiões do mundo, incluindo estratégias e planos de ação.

A proposta deste trabalho é a realização do diagnóstico da sistemática de homologação e certificação utilizada pelas empresas analisadas para homologar e certificar produtos/serviços cibernéticos. Podendo, dessa forma, contribuir cientificamente com a identificação de lacunas para que se possa formular estratégias de certificação e homologação que impliquem em um processo de desenvolvimento de produtos mais confiável sob o ponto de vista cibernético. No aspecto prático, o trabalho visa contribuir para que as empresas analisadas no estudo de caso, e organizações a elas similares, disponibilizem no mercado produtos mais adequados às necessidades estratégicas, táticas e operacionais de defesa cibernética, além de permitir a

redução das vulnerabilidades aos ataques cibernéticos e, consequentemente, a ocorrência de prejuízos financeiros para as organizações.

1.2 QUESTÕES DE PESQUISA

Este trabalho busca responder a três questões básicas:

a) Que adaptações seriam necessárias ao MRM para que possa ser aplicado em empresas cujos produtos são cibernéticos ?
b) Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho ?
c) Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho ?

1.3 OBJETIVOS

Abaixo são apresentados os objetivos do trabalho.

1.3.1 Objetivo Geral

O objetivo desta dissertação é realizar um diagnóstico da sistemática de homologação e certificação de produtos cibernéticos e identificação dos requisitos de segurança utilizados nas empresas e organismos de certificação.

1.3.2 Objetivos específicos

Para atingir o objetivo dessa dissertação são listados abaixo os seguintes objetivos específicos:

a) Identificar na literatura discussões sobre a temática defesa cibernética, assim como soluções estratégicas de segurança contra ataques de guerra cibernética para proteção de infraestruturas de TI;
b) Investigar na literatura métodos de homologação e certificação de produtos de defesa cibernética;
c) Estudar o Modelo de Referência Mecatrônico (MRM) proposto por Barbalho (2016), observando a estrutura do modelo, metodologia de aplicação, seus

processos e atividades, assim como os documentos gerados para as fases de homologação e validação de produtos;

d) Analisar os requisitos de segurança do produto propostos na Norma ISO/IEC_15408;

e) Elaborar formulários baseados nos estudos realizados que permitam o diagnóstico das metodologias de homologação e certificação de produtos de natureza cibernética em empresas desenvolvedoras desse tipo de produto assim como em órgãos públicos; além de possibilitar a identificação de práticas de segurança para o desenvolvimento do produto;

f) Identificar as lacunas entre requisitos de segurança relacionados à defesa cibernética e às práticas de homologação e certificação realizadas pelas empresas e órgãos reguladores.

1.4 JUSTIFICATIVA

Com o uso contínuo da internet e a dependência cada vez maior do ambiente de tecnologias de informação (TICs) para prestação de serviços e realização de negócios, as organizações se encontram atualmente inseridas em um ambiente de tecnologias vulneráveis a ataques cibernéticos. Muitas empresas que desenvolvem produtos/serviços tecnológicos classificados como produtos de defesa cibernética não apresentam uma padronização ou critérios de segurança eficientes para defesa cibernética. Muitas vezes esses produtos são inseridos em ambientes de infraestruturas críticas, como os órgãos centrais do estado brasileiro, sistemas financeiros, energia, telecomunicações, aeronáutica, dentre outros. Esses produtos necessitam apresentar requisitos de segurança compatíveis com esse tipo de ambiente, visando à redução dos danos causados por um ataque cibernético.

Recentes pesquisas da ISACA/RSA em conferências realizadas em 2016, demonstram que a grande maioria dos profissionais de segurança cibernética entrevistados reporta que o conselho de administração de suas respectivas empresas se preocupa com a segurança cibernética, mas somente um em cada sete diretores leva o conhecimento ao diretor executivo. A pesquisa relata ainda a ausência de percepção desses profissionais quanto aos tipos de agentes de ameaças que vem explorando a organização, não sabem informar se a organização sofreu algum ataque de ameaça persistente (APT), dentre outros. Segundo a pesquisa 61% dos entrevistados esperam um crescimento nos investimentos em segurança cibernética para o ano

de 2016 e 70% garantem que a estratégia de segurança cibernética está alinhada com o pensamento da cultura organizacional.

1.5 ESTRUTURA DO TRABALHO

O presente trabalho se encontra dividido em 5 capítulos. No segundo capítulo é realizada a revisão bibliográfica, abordando as temáticas que envolvem o estudo: cibernética, segurança cibernética, mecatrônica, processo de desenvolvimento de produtos e Modelo de Referência Mecatrônico (MRM). No capítulo 3 é discutida a metodologia de pesquisa utilizada no trabalho. No capítulo 4 são apresentadas as avaliações dos resultados. No capítulo 5 são discutidas as conclusões do trabalho, suas limitações e direcionamentos futuros.

2 REVISÃO TEÓRICA - INTRODUÇÃO AOS TEMAS PRINCIPAIS DO TRABALHO

Este capítulo tem como objetivo abordar os principais temas dentro dos quais o trabalho está inserido. O tema principal do trabalho encontra-se no processo de desenvolvimento de produtos (PDP), mais especificamente no que tange às fases de homologação e validação de produtos. É sobre essa sistemática que se justifica o desenvolvimento do trabalho e para a qual pretende agregar contribuição. A abordagem pela qual o desenvolvimento de produtos é estudada encontra-se dentro do escopo do PDP de empresas que desenvolvem produtos de Segurança de Tecnologia da Informação. Foram utilizadas normas internacionais de referência em segurança de sistemas, como a *International Organization for Standardization* (ISO), assim como o padrão internacional ISO/IEC_15408: *Common Criteria for Information Technology Security Evaluation* (2012), possibilitando definir níveis de segurança para o processo de desenvolvimento de produto, aplicáveis às fases de homologação e certificação.

Sendo assim, o capítulo apresenta uma introdução aos principais temas relacionados a esta dissertação. Na sequência: cibernética, segurança cibernética, incidente de segurança, tratamento de incidentes de segurança, mecatrônica, desenvolvimento de produtos e Modelo de Referência Mecatrônico (MRM).

2.1 CIBERNÉTICA

Neste tópico serão discutidos a origem da cibernética, infraestruturas críticas de Estado, produto cibernético como produto mecatrônico, *Cyber-Physical System* (CPS), serviços e mecanismos de segurança.

2.1.1 O que é a cibernética ?

O termo cibernética deriva do grego *kybemytiky* e originalmente significa arte de governar navios (ou homens), isto é, dirigí-los por meio da comunicação e do controle, ou seja, a arte de pilotar. No campo científico, e partindo de análises comportamentais, Wiener (1968) apresenta a cibernética como o estudo da comunicação e controle das máquinas, seres vivos e grupos sociais. A definição do termo cibernética segundo Cheng (et al., 2012) inclui a utilização de redes de computadores e comunicações e suas comunicações dentro de sistemas

empregados por instituições públicas e privadas. Barbalho et al. (2014, p. 78) definem cibernética como:

> [...] ciência que busca controlar o funcionamento de quaisquer sistemas, por meio do: (i) estabelecimento de objetivos que devem ser alcançados pelo sistema – seus parâmetros; (ii) monitoramento do funcionamento do sistema – o estado e a condição variante de suas entradas e saídas – perante os parâmetros previamente estabelecidos; (iii) tomada de decisões de controle, que visam manter o sistema dentro dos parâmetros objetivos previamente estabelecidos. Termo que se refere ao uso de redes de computadores e comunicações e suas interações dentro de sistemas utilizados por instituições públicas e privadas, [...].

A proposição inicial do conceito de cibernética, especialmente por Norbert Wiener (1968), permitiu fundamentar toda a importância de conceitos e teorias de controle, tornando elemento central no ambiente tecnológico que hoje perpassa toda a sociedade. A estratégia de segurança cibernética e de governo é alvo de estudos e de preocupação dos elementos no ambiente, dentro de um volume de tempo e espaço (BARBALHO et al., 2014).

2.1.2 Guerra cibernética

O conceito de guerra cibernética é tratado no trabalho de Parks e Duggan (2011) como um subconjunto de guerra de informação envolvendo ações dentro do mundo cibernético. O mundo cibernético, segundo o autor, compreende qualquer realidade virtual inserida dentro de uma rede de computadores. Dentre os mundos virtuais, o de maior relevância para a guerra cibernética se concentra na rede mundial de computadores e suas redes relacionadas que compartilham informações, a internet.

Muitos trabalhos têm sido desenvolvidos envolvendo o tema cibernética assim como relacionados à segurança de produtos e/ou serviços organizacionais. No trabalho de Boccardo et al. (2015), é apresentado um modelo de segurança para ambientes de avaliação e testes de *software* através da implementação de controles lógicos. No trabalho de Parks e Duggan (2011), os autores fazem uma analogia dos princípios da guerra tradicional e da guerra cibernética. Definem o mundo cibernético como um mundo artificial, criado pelo homem, utilizando *hardware* e *software*. Qualquer ação que um atacante execute neste mundo exigirá o movimento ou manipulação de dados. O espaço cibernético não é confiável ou consistente, pois nem sempre *software* e *hardware* funcionam como o esperado no espaço cibernético.

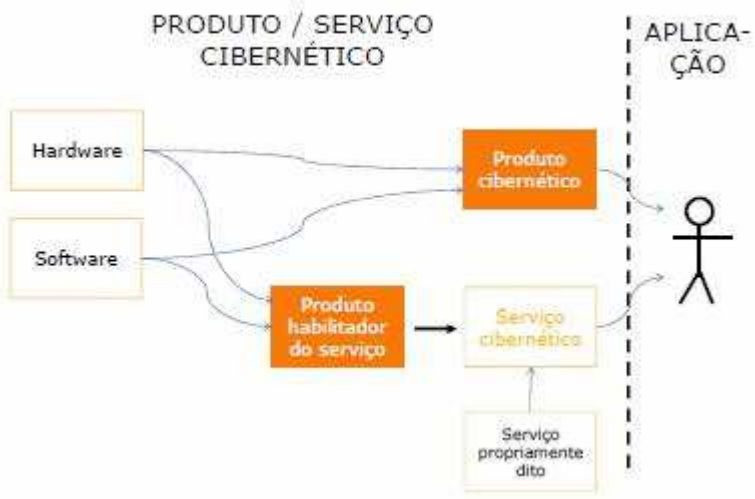
No mundo cibernético a distância física não é obstáculo à realização de ataques como acontece com a guerra humana convencional. Um ataque cibernético pode ser executado com

a mesma eficácia do outro lado do mundo, como do quarto ao lado. Com isso, percebe-se que a guerra convencional difere da guerra cibernética devido à natureza de seus ambientes, onde no primeiro o ambiente é no mundo físico enquanto o segundo é no mundo artificial, caótico e cheio de imperfeições. Muitos trabalhos têm sido desenvolvidos com grande preocupação com a guerra cibernética a nível nacional e internacional. No trabalho de Colarik e Janczewski (2011) os autores apresentam um conjunto de estratégias, normas e técnicas abordando a área política, jurídica e militar para inibição de conflitos de guerra cibernética visando à proteção das infraestruturas civis e militares, proprondo um ambiente colaborativo e abrangente de segurança.

2.1.3 Produto cibernético

Produto cibernético pode ser definido como um “Conjunto de atributos tangíveis ou intangíveis necessários para manter infraestruturas críticas em níveis seguros e que seja capaz de prevenir e detectar incidentes como forma de proteção aos sistemas cibernéticos por meio de *hardware* e *softwares* seguros” (BARBALHO et al. 2014, p. 74). Já o conceito de produto cibernético de defesa, pode ser considerado conforme a Portaria do Ministério da Defesa Nº 3.229/13 como um tipo de Produto Estratégico de Defesa (PRODE), que é todo aquele que, pelo conteúdo tecnológico, pela dificuldade de obtenção ou pela imprescindibilidade, seja de interesse estratégico para a defesa nacional. Dessa forma entende-se que o produto de defesa cibernética é um produto cibernético. Um exemplo de produto cibernético são os “drones”, nome genérico e amplo são utilizados para descrever desde pequenos multirrotores rádio-controlados de uso recreativo até os Veículos Aéreos Não Tripulados (VANT) de aplicação militar. Já o termo Aeronave Remotamente Pilotada (RPA) é considerado um tipo de VANT com a presença de um piloto remoto responsável pela operação segura da aeronave. Existem ainda os Sistemas de Aeronave Remotamente Pilotadas (RPAS) que apresentam um certo grau de autonomia (AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL).

Figura 1 – Produto/Serviço cibernético



Fonte: BARBALHO et al., 2014.

Conforme é exibido na Figura 1, um produto ou serviço cibernético pode ser constituído de componentes de *hardware* e/ou *software* para atender a uma determinada aplicação, como por exemplo, um equipamento de chaves encriptadas, que é baseado em *hardware* e *software*. Em outros casos, pode-se ter um produto acompanhado de um serviço de atualização de antivírus, visando à rapidez de proteção frente aos principais *malwares* lançados. O serviço propriamente dito, representado na Figura 1, na verdade representa a atualização de *software*.

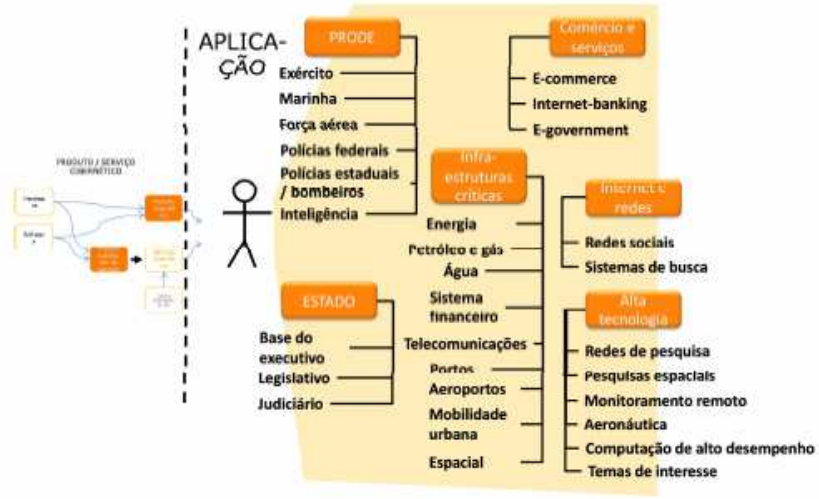
Há também outros serviços os quais não demandam a aquisição de um produto específico, sendo uma prática comum no mercado de produtos cibernéticos a entrega gratuita do serviço com base em um modelo de negócios fundamentado publicamente na propaganda e na publicidade. Dessa forma, o serviço será provido baseado em um *hardware* habilitador, como é o caso dos serviços de e-*mail Gmail* ou *Yahoo*, as buscas do Google, as redes *Facebook*, *Twitter*, *Linkedin*. Serviços estes que, para serem utilizados, dependem de outros produtos como o *browser* de internet, a infraestrutura de redes locais da empresa, tanto em termos de *hardware* como de *software*, e os próprios computadores, ou seja, esses produtos habilitadores apresentam componentes de *hardware* e *software*. O serviço prestado envolve ainda uma série de procedimentos, como o cadastro de usuários, senhas de acesso, níveis de utilização, dentre outros.

Considerando o âmbito que envolve este cenário, o produto de defesa cibernética também apresenta as mesmas características e ou comportamento em relação a *hardware*,

software e serviços dos produtos de aplicação geral. Surge com isso a necessidade dessa base técnica passar por um processo de certificação e homologação demonstrando que não há intrusão, *backdoor* ou bomba lógica que possa capturar dados do sistema ou o torne inoperante, ou ainda que cause restrição de sua operacionalidade. Esse processo de segurança tanto do produto como do serviço prestado sob o ponto de vista cibernético, será discutido no tópico Segurança Cibernética.

A Figura 2 mostra o ambiente de aplicação do produto cibernético, assim como possibilita ter uma noção inicial dos usuários de um sistema de defesa cibernética. Para estes usuários o produto cibernético precisa ser seguro tanto no que tange ao aspecto de *software* como ao *hardware* acompanhado de *software*, bem como o serviço prestado de defesa cibernética precisa estar isento de vulnerabilidades de *hardware* e de *software*, evitando possíveis espionagens por parte de outros países.

Figura 2 - Ambiente de aplicação de produtos de defesa cibernética



Fonte: BARBALHO et al., 2014

Os órgãos centrais do Estado brasileiro são usuários importantes desse tipo de produto e/ou serviço. O Palácio do Planalto precisa ser seguro especialmente em termos de *software* e telecomunicações. O corpo diplomático precisa estar também envolto a um ambiente de TIC (tecnologias de informação e comunicação) seguro, podendo ser replicado ao Congresso, ao Senado e à Justiça Federal (BARBALHO et al. 2014).

2.1.4 Infraestruturas Críticas do Estado

As denominadas infraestruturas críticas do Estado e Sociedade são outros elementos a serem considerados sob o ponto de vista de usuários de serviços e produtos seguros do ponto

de vista cibernético. Tais infraestruturas podem ser objeto de ataques cibernéticos como os mencionados pelo Governo americano. A lógica básica de segurança é que o sistema de controle de uma usina hidrelétrica que provê energia para milhões de pessoas pode, se for vulnerável a ataques cibernéticos, ser causa de prejuízos econômicos de grandes proporções, ou se o país estiver envolvido em um conflito armado, ser atacado para provocar caos nas cidades e impossibilidades de manutenção de serviços básicos para a população, a indústria e os próprios órgãos de defesa (FERNANDES, 2012).

Dentre as infraestruturas críticas se encontram as empresas de energia que são vulneráveis a ataques de *Hackers* e *Crackers*, tanto nos equipamentos e TIC utilizados como também nos seus sistemas de transmissão e repartição de energia, salas de controle e simulação virtual. No caso de geração de energia, mais especificamente, há demanda tanto por *hardware* como por *software* e serviços que implicam em riscos de natureza cibernética. Outras empresas vulneráveis seriam as de abastecimento de água, com alto impacto sobre as populações usuárias.

O Sistema Financeiro entra como um dos mais críticos e que, estatisticamente, é o que mais sofre ataques com fraudes internas (funcionários e trabalhadores da empresa) e externas, isto é, criminosos que tentam burlar seus sistemas para obter ganhos financeiros ocasionando prejuízos tanto para a empresa quanto aos seus clientes. Embora o maior impacto seja de *software* dado o grande conjunto de operações atualmente realizadas pela internet, há também importantes infraestruturas de *hardware* de comunicações e de informática e controle de redes.

Os Sistemas de Telecomunicações talvez sejam os subsistemas mais vulneráveis dentre os das infraestruturas críticas. As estruturas que suportam esse sistema no Brasil devem apresentar normas e leis que zelem pela segurança do sistema, inclusive pela sua importância e no impacto que o mesmo exerce nos demais. Os Sistemas de transporte também estão sujeitos a ataques cibernéticos, devendo ser periodicamente avaliados com seus equipamentos e constantemente monitorados, incluindo os sistemas de sinalização eletrônica, sistemas inibidores de velocidade e câmeras de observação de tráfego, dentre outros. A área espacial também é um tipo de infraestrutura crítica, estando no estado da arte da tecnologia de diversas áreas, como computação, aeronáutica, ciências aeronáuticas, dentre outras, utilizando sistemas críticos, tanto de *hardware* como de *software* (BARBALHO et al., 2014).

Outro tópico importante a ser mencionado são as aplicações vinculadas ao comércio eletrônico, tanto de empresas do grande varejo, como a segurança de internet *banking* e *e-*

government. Com o grande aumento do volume de serviços e produtos que são utilizados através da internet, aumenta também a necessidade de que este ambiente possa oferecer segurança, tanto a nível de *hardware* de comunicação e de processamento de dados quanto no aspecto *software* e serviços. A grande maioria das empresas que oferecem serviços de redes sociais é americana, e o grande volume de informações pessoais, de estilo de vida, de relacionamentos dos mais diversos, de preferências de consumo preocupa cada vez mais a Comunidade Europeia no que tange à gestão da informação disponível na rede, sob o ponto de vista cibernético (BARBALHO et al., 2014).

2.1.5 Produto Cibernético como Produto Mecatrônico

Os produtos mecatrônicos podem ser considerados essencialmente cibernéticos conforme as definições encontradas em Wiener (1984), uma vez que a ciência da cibernética é considerada como ciência da comunicação e controle, permitindo fundamentar vários conceitos, como dos dispositivos de sensoriamento e atuação, conforme Barbalho (et al., 2014). Em linhas gerais um produto mecatrônico deve apresentar alguns critérios como os descritos por Bradley (1991):

a) Integração de tecnologias mecânica, eletrônica e de *software;*
b) Funções básicas do produto devem ser providas pela interação entre as tecnologias que o compõem;
c) O produto deve ser entendido como um sistema de controle de malha aberta ou fechada.

Segundo Buur e Andreasen (1990) “Mecatrônica é uma tecnologia que combina mecânica com eletrônica e tecnologia da informação para compor tanto uma interação funcional como uma interação espacial de componentes, módulos, produtos e sistemas”.

Assim, é possível encontrar uma variedade de produtos cibernéticos com características mecatrônicas fornecendo segurança em um ambiente de TIC. Dentre eles, pode-se destacar o próprio computador (*desktop*), quando instalado com programas de proteção ou inserido em um ambiente de segurança física ou lógica, *Virtual Private Network* (VPN), *Firewalls*, *Intrusion Detection Systems* (IDS).

2.1.6 Sistemas Físicos Cibernéticos

A visão da indústria 4.0, ou Quarta Revolução Industrial traz o conceito dos Sistemas de produção *Cyber-Physical System* (CPS), caracterizados pela inteligência descentralizada com a comunicação máquina a máquina (M2M). A tendência da evolução dos sistemas de controle industrial é se tornarem cada vez mais complexos e distribuídos, o que possibilitará um processo flexível e minucioso (SAT AUTOMAÇÃO INDUSTRIAL, 2016).

Os CPS podem ser definidos como sistemas inteligentes que incluem redes de componentes físicos e computacionais. Esses sistemas altamente conectados e integrados provêem novas funcionalidades para melhorar a qualidade de vida e habilitar avanços tecnológicos em áreas críticas, tais como assistência médica personalizada, gestão de tráfego, manufatura inteligente, defesa e segurança, e suprimento e uso de energia. Outros termos são utilizados para transmitir conceitos similares ou relacionados, tais como internet industrial, internet das coisas (*Thing Internet* ou IoT), *machine-to-machine*, cidades inteligentes, etc (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2016).

Podem ainda ser considerados uma combinação das capacidades dos sistemas embarcados e sua capacidade de comunicação através de múltiplas tecnologias, o que permite a aplicação de CPS em sistemas de produção, transporte e logística.

Além disso, os CPS destacam-se pela possibilidade de combinação dos aspectos cibernéticos de processamento e comunicação com os aspectos dinâmicos e materiais dos sistemas físicos (RAJKUMAR, 2012). Uma das grandes preocupações dos governos das principais potências mundias segundo Barbalho et al. (2014) tem sido a dependência existente quanto à informação envolvida nos CPS. Conforme o padrão americano, as características diferenciadoras dos CPS incluem, dentre outras:

a) Para o funcionamento do CPS é essencial a combinação do espaço cibernético e do físico, provendo um ambiente integrado;
b) os dispositivos podem ser adaptados a diferentes aplicações, o que leva a implicações importantes no projeto;
c) algumas questões devem ser consideradas quando se trata de CPS, devido à sua capacidade de interação com o mundo físico. Dentre elas estão a confiabilidade, resiliência, segurança da informação, privacidade e garantia de controle de intrusão são críticos;

d) considerando que as soluções CPS podem ser baseadas em serviços outros elementos de segurança devem ser considerados como a confidencialidade, privacidade, segurança, integridade, não repúdio, dentre outros.

Tang et al. (2013) sugerem técnicas para acelerar algoritmos para aumentar a confiabilidade dos dados de sensores em CPS. Um grande desafio para os CPS é a confiabilidade dos mesmos devido a algumas dificuldades elencadas abaixo:

a) Dados com ruído: muitos experimentos apresentam grande dificuldade na obtenção de dados precisos em aplicações que utilizam CPS;
b) Falhas podem ocorrer de formas imprevisíveis e menos de 49% de seus dados poderiam ser utilizados para interpretação significativa;
c) Conflitos entre sensores: um sistema CPS bem implantado apresenta redundâncias razoáveis e cada região é monitorada por diferentes sensores e muitas vezes, um sensor pode não funcionar corretamente, mas outros ainda podem fornecer informações precisas. Nesse caso, os conflitos ocorrem entre sensores confiáveis e defeituosos;
d) Incerteza dos objetos: os alarmes em sistemas CPS são causados por comportamentos anormais na região monitorada, por exemplo, um ataque a um sistema em rede. Devido a limitações de *hardware*, os sensores podem não fornecer informações detalhadas sobre os objetos da invasão. A maioria deles só pode estimar uma possível região dos objetos. O sistema precisa integrar dados de vários sensores para estimar a informação detalhada do objeto.

2.1.7 Ataques, Serviços e Mecanismos de Segurança

A classificação de ataques utilizada tanto na ITU-T X.800 quanto na RFC 2828 se baseia na separação em termos dos passivos e ativos. Um ataque passivo pode ser definido como a tentativa de descoberta ou utilização de informações do sistema, sem afetar os recursos. Já os ataques ativos, a tentativa é de conseguir alterar os recursos do sistema ou afetar sua operacionalidade (STALLINGS, 2010).

Dentre os tipos de ataques passivos estão a liberação do conteúdo da mensagem e análise de tráfego. Considerando as categorias de ataques do tipo ativos, podem-se citar: disfarce, repetição, modificação e negação de serviço. Alguns mecanismos de segurança

sugeridos pela arquitetura ITU-T X-800 podem ser adotados pelas organizações para proteção dos seus ativos. A referida arquitetura define um serviço de segurança como sendo um serviço provido por uma camada de protocolo de comunicação de sistemas abertos, garantindo a segurança adequada dos sistemas ou das transferências de dados. Já a RFC 2828 define serviço de segurança como de processamento ou de comunicação prestado por um sistema para fornecer um tipo específico de proteção aos recursos do sistema. A X-800 divide os serviços em 5 categorias e 14 serviços específicos:

a) Autenticação;
b) Controle de Acesso;
c) Confidencialidade dos dados:
    a. Confidencialidade da conexão;
    b. Confidencialidade sem conexão;
    c. Confidencialidade por campo seletivo;
    d. Confidencialidade do fluxo de tráfego.
d) Integridade dos dados:
    a. Integridade da conexão com recuperação;
    b. Integridade da conexão sem recuperação;
    c. Integridade da conexão com campo seletivo;
    d. Integridade sem conexão;
    e. Integridade sem conexão com campo seletivo.
e) Irretratabilidade:
    a. Irretratabilidade, Origem;
    b. Irretratabilidade, Destino.

Os mecanismos de segurança recomendados pela X-800 são divididos entre os implementados em uma camada específica de protocolo e nos específicos a qualquer camada de protocolo ou serviço de segurança em particular.

a) Mecanismos de Segurança Específicos:
    a. Cifragem;
    b. Assinatura Digital;
    c. Controle de Acesso;
    d. Integridade dos Dados;

e. Troca de Informações de Autenticação;
f. Preenchimento de Tráfego;
g. Controle de Roteamento;
h. Certificação.

b) Mecanismos de Segurança Pervasivos:
a. Funcionalidade confiável;
b. Rótulo de Segurança;
c. Detecção de Evento;
d. Registros de Auditoria de Segurança;
e. Recuperação de Segurança.

2.2 SEGURANÇA CIBERNÉTICA

Nesse tópico serão discutidas as abordagens existentes para o entendimento da segurança cibernética, incluindo legislação correlata e trabalhos desenvolvidos na área. Além disso, serão apresentadas soluções estratégias de defesa cibernética pesquisadas na literatura.

2.2.1 Abordagens para o Entendimento da Segurança Cibernética

É possível encontrar discussões acerca da segurança cibernética em literaturas relacionadas às disciplinas de inteligência artificial, máquina de vetores, matemática, processos estocásticos, segurança da informação, redes de computadores, gestão da segurança, dentre outras. No trabalho de Al-Ahmad (2013) são apresentadas soluções estratégicas de segurança contra ataques de guerra cibernética para proteção de infraestruturas de TI, tanto para o setor público como para o privado. Conforme o autor, as soluções devem ser revisadas periodicamente para lidar com novas ameaças e mudanças tecnológicas. Em inteligência artificial existem trabalhos para a segurança do sistema de transporte rodoviário de materiais perigosos.

Alguns autores como Berman, Drezner e Wesolowsky (2000) desenvolveram algoritmos e heurísticas para resolver o problema de roteamento de veículos para minimizar a exposição da população em casos de acidentes. Em matemática há recente desenvolvimento de análise estocástica para a identificação de ataques cibernéticos em um dado intervalo de tempo. Através da utilização da função de distribuição de Erlang, Daras (2014) estima o total de ocorrências de ataques cibernéticos em um sistema cibernético. Ainda na matemática, Walden

e Kaplan (2004) utilizaram a abordagem bayesiana para estimar o tamanho e o tempo de um ataque de vírus antraz para determinar o número de pessoas que necessitavam de cuidados médicos.

Na área de segurança de fronteiras em companhias aéreas Wein e Baveja (2005) estudaram o programa de visitantes dos EUA que tem como objetivo a redução de fraudes em vistos e detecção da entrada de suspeitos e criminosos. Este programa utiliza um modelo baseado na teoria dos jogos para análise da qualidade de impressões digitais. Outros trabalhos na área de segurança de companhias aéreas, como o de Barnett (2004), utilizam modelos dinâmicos de probabilidade e técnicas de mineração de dados para classificação de ameaças aos passageiros.

Na área de engenharia elétrica, visando minimizar a indisponibilidade do serviço público de energia elétrica, Baskerville e Portougal (2003) desenvolveram um modelo que estima um período ótimo de tempo, onde a possibilidade de ataques à infraestrutura do sistema seja mínima. Através de decomposição foi utilizado técnicas de heurística e pesquisa em segurança cibernética para ajudar a previnir, proteger, detectar e se recuperar de ataques cibernéticos em infraestruturas de informação, Salmeron, Wood e Baldick (2004); Tinnel, Saydjari e Farell (2002) definem conceitos e táticas de estratégia cibernética para ajudar a determinar as melhores ações a serem tomadas durante situações de um ataque cibernético. É elaborada uma cartilha de apoio e defesa de infraestruturas críticas para o setor público. No trabalho de Daras (2014) é utilizada a análise estocástica para determinar o número esperado de ataques cibernéticos em um intervalo de tempo, assim como poder estimar o momento mais propício de ocorrência dos mesmos. O autor utiliza funções de distribuição para suas estimativas, como, por exemplo, a função de *Erlang* e a função de *Bernoulli.*

Para proteção da infra-estrutura cibernética nas organizações o trabalho de Sharma (2010) apresenta um planejamento de estratégias para a guerra cibernética baseado em camadas de defesa e redundância. O autor define uma fase inicial chamada de pré-conflito, onde são definidos procedimentos para iludir atacantes e moldar futuros conflitos. Uma segunda fase intermediária denominada conflito é composta por duas subfases: agir e dominar e uma última fase denominada de pré-conflito. Apesar de todos os esforços para proteção do ambiente, o autor comenta que não há garantia da segurança em sentido amplo, até o momento em que seja encontrada uma nova vulnerabilidade.

A falta de uma padronização em segurança cibernética assim como o compartilhamento de informações pertinentes às estratégias adotadas é um problema enfrentado por muitos

países, conforme mostra o trabalho de Shafqat e Massod (2016), no qual os autores realizam uma comparação das estratégias nacionais de segurança cibernética em 20 países de diferentes regiões do mundo. Relatam ainda a Malásia como o país mais experiente em cibernética, porém, assim como o Irã e Israel, não compartilham suas estratégias de segurança cibernética.

Segundo os autores, o conceito de espaço cibernético para países como Nova Zelândia, Austrália, Alemanha, Espanha e Canadá refere-se apenas à internet e aos dispositivos de TIC pertinentes. As estratégias de quase todos os países são documentadas e, apesar de metas e objetivos semelhantes, a pesquisa revelou inúmeras diferenças no âmbito e na abordagem das 20 estratégias selecionadas para o estudo. Conclui-se que as estratégias do Reino Unido, EUA e Alemanha são particularmente mais estruturadas do que os outros países em termos de desenvolvimento e execução de planos de ação, considerando as seguintes métricas: documentação das estratégias de segurança cibernética, nível de priorização atribuído à segurança cibernética, percepção do País das ameaças cibernéticas, capacidade de resposta a incidentes e capacitação.

Alguns padrões da indústria como o *Payment Card Industry Data Security Standard* (PCI DSS), contribuem para a adoção de controles de segurança, porém o caminho ainda é árduo. Quando um produto é disponibilizado no mercado ou um serviço é prestado, é necessário que os mesmos tenham qualidade, assim como a segurança, deve ser considerada como um pré-requisito do processo de negócio das organizações. O grande diferencial que proporcionará confiança às organizações frente ao mercado será baseado no conceito de que é preciso “funcionar com segurança” (NAKAMURA; GEUS, 2007).

Como as organizações poderiam prover segurança para produtos tão complexos, como os cibernéticos ? Que modelo de homologação e certificação poderá ser aplicado em empresas cujos produtos são cibernéticos ? É essa lacuna existente na literatura em relação à padronização para o desenvolvimento de produtos cibernéticos que este trabalho busca suprir. Os produtos mecatrônicos podem ser considerados essencialmente cibernéticos devido às características presentes, o que permite a viabilização de utilização do MRM proposto por Barbalho (2006) para suporte ao desenvolvimento desses produtos.

No trabalho de Min, Chai e Han (2015) os autores realizam um estudo comparativo internacional das estratégias de segurança cibernética adotadas pelos EUA, Japão e União Européia. Nos EUA existe um conselho de segurança nacional que controla, dirige e implementa a política nacional de segurança cibernética. Porém ainda não foi definida uma lei específica para tratar do tema. Por outro lado, a União Européia possui planos de ação em

diversas áreas, dentre as quais o governo definiu sete planos como prioritários, incluindo a segurança cibernética.

Os autores relatam que no ano de 2005 o Japão estabeleceu o Centro Nacional de Segurança da Informação (NISC), sob a autoridade do governo e a criação de níveis de segurança para infraestruturas críticas; em 2013 inaugurou a Estratégia de Segurança Cibernética, ampliando a área de proteção para o espaço cibernético. Os autores relatam que os países analisados possuem estratégias sob a ótica da Segurança Cibernética, mas ainda é necessário reforçar a parceria público-privado, pois a grande maioria utilizadora do espaço cibernético são empresas privadas. O desenvolvimento de tecnologias da informação e comunicação expõem as empresas a ameaças cibernéticas. Os autores relatam as questões que envolvem o tema cibernética são difíceis de se resolverem por completo.

No trabalho de Coelho e Silva (2013) é apresentada uma proposta para certificação de equipamentos de tecnologia da informação, permitindo prover um ambiente de segurança e confiabilidade. A proposta é baseada na existência de um laboratório de certificação baseado na norma ISO/IEC-17025 (ABNT, 2005) e os resultados desses testes e avaliações são incluídos em um relatório técnico, acreditado por organismos internacionais. A garantia do nível de confiabilidade obtida deverá assegurar que o equipamento esteja livre de quaisquer ameaças cibernéticas.

2.2.2 Legislação e Normas Técnicas

Algumas normas relacionadas abaixo servem como referência para questões pertinentes a padronização de produtos e serviços, desenvolvimento de produtos/sistemas seguros para TICs, assim como cita alguns padrões, serviços e protocolos oficiais da *Internet*. Além disso, outras normas abordam questões aplicáveis às organizações quanto ao desenvolvimento de um SGSI (Sistema de Gestão de Segurança da Informação), definindo mecanismos de controle e riscos na segurança da informação. Neste trabalho foram utilizadas as seguintes Normas: ISO/IEC-15408 e IEEE 1012-2012.

2.2.2.1 ABNT (Associação Brasileira de Normas Técnicas)

Órgão responsável pela normalização técnica no país, fundada em 1940, fornece a base necessária ao desenvolvimento tecnológico brasileiro.

a) ABNT/CB-08 - Comitê Brasileiro de Aeronáutica e Espaço: a referida norma apresenta âmbito de atuação no campo aeroespacial, compreendendo materiais, componentes, equipamentos, projeto, fabricação, avaliações, manutenção de subsistemas de aeronaves e veículos espaciais; bem como materiais, equipamentos e manutenção em infraestrutura aeroespacial, no que concerne à terminologia, requisitos, métodos de ensaio e generalidades.

2.2.2.2 ISO (International Organization for Standardization)

A *International Organization for Standardization* (ISO) é uma organização mundial de normalização que apresenta os seguintes objetivos: aprovação de normas internacionais em todas as áreas técnicas, como normas técnicas, especificações técnicas (TS) e relatórios técnicos (TR) relacionados a procedimentos e processos que visam a padronização de produtos e serviços, assim como, no tocante à segurança da informação, a garantia da confiabilidade, da segurança e da qualidade dos produtos e serviços produzidos por uma empresa.

A ISO oferece um conjunto amplo de normas que atendem às exigências dos negócios, às necessidades do consumidor, sociedade e usuário final. Dentre elas estão as normas de apoio ao desenvolvimento deste trabalho, tais como:

a) **ISO 19011:2012:** Diretrizes para auditoria em sistemas de gestão. Fornece orientações acerca de auditorias em sistemas de gestão;
b) **ISO 9000:2005:** Sistemas de gestão da qualidade. Aborda o conceito de gestão da qualidade (fundamentos e vocabulário) para implementação e operação em empresas;
c) **ISO 9001:2015:** Gestão da qualidade). Aborda sistemas de gestão da qualidade publicada em versão *Draft International Standard* (DIS), atualizada com as práticas e necessidades do mercado.

2.2.2.3 IEC (International Electrotechnical Commission)

A *International Electrotechnical Commission* (IEC) é uma organização mundial líder na preparação e publicação de normas internacionais coletivamente conhecidas como “eletrotecnologia”, abrangendo as áreas de eletrônica, elétrica e tecnologias associadas na

terra, no mar e no ar. Ela escolhe especialistas que atuam em vários segmentos de mercado, órgãos governamentais, associações para participarem do trabalho de avaliação técnica. Tem como objetivo harmonizar as opiniões de especialistas de todo o mundo visando assegurar a fabricação de produtos e serviços seguros.

Em aplicações *web* existem um conjunto de normas ISO/IEC que tem como objetivo o gerenciamento de vulnerabilidades apoiando as melhores práticas de Gestão da Segurança da Informação:

a) **ISO/IEC-27001:** Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Norma que trata da definição de técnicas para o desenvolvimento de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações;
b) **ISO/IEC-27002:** Código de Prática para a Gestão da Segurança da Informação. Esta norma é uma complementação da ISO/IEC-27001, que estabelece mecanismos de controle para o SGSI e aborda um conjunto de especificações e melhores práticas para iniciar, implementar e manter o SGSI;
c) **ISO/IEC-27005**: Gestão de Riscos de Segurança da Informação. Esta norma trata da Gestão de Risco na Segurança da Informação (*Information Security Risk Management*) fornecendo diretrizes para conduzir e colaborar com a implantação de processos de Segurança da Informação com base na abordagem de Gestão de Risco, e em conformidade com os conceitos gerais especificados nas respectivas normas: ISO/IEC 27001 e 27002;
d) **ISO/IEC-15408**: *Common Criteria for Information Technology Security Evaluation* (2012). Essa norma é uma referência para desenvolvedores, administradores e auditores de segurança para sistemas de informação. Tem como objetivo avaliar a segurança de produtos de TI de acordo com níveis de segurança, definidos como *Evaluation Assurance Level* (EAL1 a EAL7).
e) **ISO/IEC-17025**: Requisitos gerais para a competência de laboratórios de ensaio e calibração. Essa norma aborda os requisitos para acreditação de laboratórios.

2.2.2.4 ISO/IEC-15408 - Common Criteria for Information Technology Security Evaluation

O Common Criteria é um *framework* utilizado como padrão internacional que define critérios comuns de padrão de avaliação da Segurança da Informação ISO/IEC_15408, para a

segurança de computadores. Tem como objetivo avaliar a segurança de produtos de tecnologia de acordo com diversos níveis de segurança, definidos como *Evaluation Assurance Level* (EALs).

Dessa forma um produto é classificado em um nível (EAL1 a EAL7), a partir da análise das técnicas de especificação e desenvolvimento que foram empregadas na sua construção e da avaliação do produto no cumprimento dos requisitos de segurança especificados. No nível mais alto de certificação, exige-se a utilização de métodos formais e o seu relacionamento com a especificação de políticas de segurança.

O CC é um guia de desenvolvimento para produtos e sistemas seguros, podendo suas medidas serem aplicáveis à segurança em *hardware, firmware ou software*. Seu escopo encontra-se alinhado aos conceitos da política de segurança como confidencialidade, integridade e disponibilidade da informação.

O objetivo da segurança é a proteção dos ativos organizacionais (*assets*), das ameaças (*threats*), ou seja, a utilização indevida dos mesmos. São então, inseridos procedimentos de contramedidas (*countermeasures*) para que se consiga anular as vulnerabilidades (*vulnerabilities*) e consequentemente, mitigar os riscos ao ambiente.

O CC é dividido em 3 partes, sendo que a Parte 1 (*Introduction and general model*) fornece uma introdução e visão geral do modelo; a Parte 2 (*Security functional components*) define a segurança para os componentes funcionais; e a Parte 3 (*Security assurance components*) define os componentes de garantia de segurança.

2.2.2.5 RFC (Request for Comments)

Algum documentos de referência, conhecidos como RFC (*Request for Comments*), são publicações que documentam os padrões, serviços e protocolos oficiais da Internet, são mantidos pelo *Internet Engineering Task Force* (IETF).

a) **RFC 2196**: Esta RFC descreve políticas e procedimentos de segurança para sites com sistemas na Internet, sendo um guia prático aos gestores;
b) **RFC 2350**: *Expectations for Computer Security Incident Respons.*
c) **Norma Complementar nº 05/09**: Disciplina a criação de equipe de tratamento e resposta à incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta.

*2.2.2.6 IEEE (*Institute of Electric and Electronic Engineers*)*

O Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) é uma organização profissional fundada em 1963 nos Estados Unidos, cuja meta é fomentar os conhecimentos na área da engenharia elétrica, eletrônica e da computação, sendo considerada líder no desenvolvimento de normas internacionais de suporte à telecomunicações, tecnologia da informação e produtos e serviços de geração de energia.

A Norma IEEE 1012-2012: *Standard for System and Software Verification and Validation* (IEEE, 2012) é utilizada para verificação e validação de processos para determinar se os produtos desenvolvidos estão em conformidade com as exigências da referida atividade e se os mesmos atendem aos requisitos do cliente (usuário). A abrangência dos processos inclui sistemas, *software* (*firmware* e microcódigo) e *hardware* que estão sendo desenvolvidos, incluindo suas interfaces. Os processos (V & V) incluem análise, avaliação, revisão, inspeção e testes de produtos. A referida norma foi utilizada como base para elaboração de perguntas sobre os procesoss de verificação e validação de *software* no Formulário de Análise do Processo de Homologação do Produto (APÊNDICE A).

2.2.2.7 Metodologia de avaliação CERTICS

A certificação do produto segundo a Metodologia de Avaliação da CERTICS para *software*, viabiliza as condições de preferência em compras públicas. A Metodologia segue as seguintes diretrizes: a avaliação é do *software* e não da empresa, baseando-se na análise dos processos utilizados no *software;* no conjunto de normas ISO/IEC 15504 (ABNT, 2008) e na experiência do Centro de Tecnologia da Informação Renato Archer (2013). A Metodologia apresenta um conjunto mínimo de resultados esperados e nenhuma forma específica de estruturação, operação e documentação são exigidas da organização solicitante. A Metodologia é composta por dois componentes principais: (1) Modelo de Referência para Avaliação CERTICS e (2) Método de Avaliação da CERTICS (ALVES; SALVIANO; STEFANUTO, 2015).

O Modelo de Referência CERTICS (ALVES; SALVIANO; STEFANUTO, 2015) possui uma arquitetura a qual é estruturada em quatro camadas: (1) Conceito Fundamental, ou seja, *software* resultante de desenvolvimento e inovação tecnológica realizados no País; (2) Áreas de Competência: Desenvolvimento Tecnológico (DES), Gestão de Tecnologia (TEC), Gestão de Negócios (GNE), e Melhoria Contínua (MEC). Cada área envolve tanto aspectos de

competências tecnológicas quanto competências correlatas e um conjunto de resultados esperados; (3) Resultados Esperados, a qual detalha cada uma das Áreas de Competência; e (4) Orientações e Indicadores, a qual detalham os Resultados Esperados definidos na camanda anterior. Baseado nas orientações e indicadores utiliza-se uma pontuação definida na Norma ISO/IEC_15504-2: (F) Completamente atendido; (L) Largamente atendido; (P) Parcialmente atendido e (N) Não atendido.

O Método de Avaliação da CERTICS (ALVES; SALVIANO; STEFANUTO, 2015) orienta a avaliação de um *software*, para determinar se o mesmo é resultante de desenvolvimento tecnológico e inovação tecnológica no País, sendo composto por seis fases: F1) Exploração; (F2) Contratação; (F3) Preparação; (F4) Visita; (F5) Validação e (F6) Conclusão. O resultado é validado e comunicado à organização, sendo positivo será enviado à SEPIN/MCTI que é a responsável pela emissão e publicação do certificado no Diário Oficial da União (DOU). O referido modelo é adotado pela Empresa A do estudo de caso para certificação de seus produtos.

2.2.2.8 Metodologia de avaliação CESVI Brasil

O CESVI BRASIL (Centro de Experimentação e Segurança Viária) atua no campo de segurança viária, desenvolvimento de estudos e campanhas além de prestar serviços a órgãos do governo, incluindo regulamentações pertinentes ao trânsito e ao automóvel. Além disso, é responsável pela certificação nos sistemas de segurança do veículo como os rastreadores de veículos, através de análise técnica profunda. Possui um laboratório para análises técnicas, realização de testes práticos em equipamentos embarcados, análise de interferências, consumos, tráfego de informações e funcionalidades dos sistemas.

Além disso, a avaliação de bloqueadores e rastreadores da CESVI BRASIL inclui a análise da estrutura da empresa, equipamentos, processos, qualidade da instalação, mão de obra e eficiência do produto. A certificação desenvolvida pelo Centro verifica em sua metodologia de avaliação, itens como: Legalidade e Certificações, Instalação de Equipamentos, Assistência ao Veículo, *Software*, Funcionamento do equipamento, Formação de operador logístico junto ao *software*, Sistemas de Comunicação e Central de Atendimento.

2.3 INCIDENTE DE SEGURANÇA

Neste tópico serão citados alguns órgãos responsáveis pela segurança da internet brasileira e discutidos alguns conceitos relacionados à segurança, incluindo incidentes de segurança, tratamento de incidentes, ameaças no ambiente, riscos e vulnerabilidades futuras.

2.3.1 Definição de Incidente de Segurança

O termo Incidente de Segurança refere-se a qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Dentre eles podem ser mencionadas as tentativas de acesso não autorizado a sistemas, modificações sem consentimento prévio, dentre outros.

2.3.2 *CERT.br* (Centro de Estudos para Resposta e Tratamento de Incidentes)

O termo CERT.br refere-se a um Centro de Estudos para Resposta e Tratamento de incidentes para a internet brasileira, mantido por um Núcleo de Informação e Coordenação do Ponto BR, o NIC.br. A função do referido núcleo é a implementação das decisões e dos projetos do Comitê Gestor da Internet no Brasil, o CGI.br, que por sua vez é o responsável pela coordenação e integração das iniciativas e serviços da internet no País. O grupo CERT.br é responsável pelo tratamento de incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua centralizando as notificações de incidentes de segurança no Brasil, provendo coordenação e apoio às respostas de incidentes (ALBERTS et al., 2004). Dentre as principais atividades realizadas pelo CERT.br, são elencadas as seguintes:

a) Oferecer suporte adequado ao processo de recuperação e análise de ataques e de sistemas comprometidos;
b) estabelecer cooperação com entidades provedoras de acesso e serviços de Internet;
c) manter um arquivo de estatísticas dos incidentes tratados assim como das reclamações de *spam* recebidas;
d) oferecer treinamentos na área de tratamento de incidentes de segurança;
e) determinar as tendências de ataques no espaço de Internet Brasileiro;
f) obter dados sobre o abuso da infraestrutura de redes conectadas à Internet.

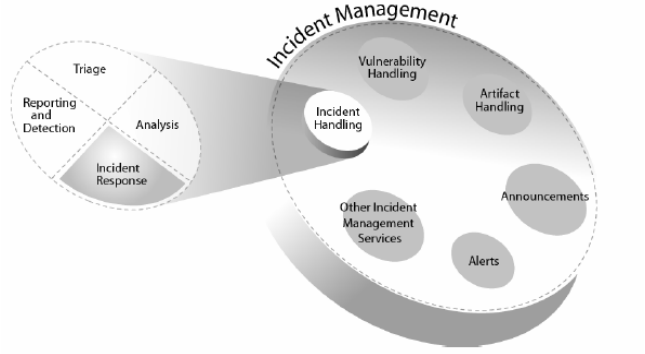
2.3.3 CSIRT (Computer Security and Incident Response Team)

O termo CSIRT em Cabrera et al. (2010) refere-se a um grupo de Segurança e Resposta a incidentes que tem como finalidade o fornecimento de serviços para gestão de incidentes de informática, para uma determinada empresa particular. Seu trabalho é semelhante a respostas de serviços de emergência, sendo necessário possuir as ferramentas adequadas e os planos necessários para prover uma resposta eficaz e responder de forma proativa, evitando catástrofes, sempre que possível. Dentre os serviços oferecidos pelo CSIRT, podem ser encontrados os listados abaixo:

a) **Serviços Reativos**: Tratamento de incidentes, detecção e rastreamento de invasões, análise de artefatos/vulnerabilidades;
b) **Serviços Proativos**: Configuração e manutenção dos sistemas, desenvolvimento de ferramentas, provimento de documentação e orientação.
c) **Serviços de Gestão da Qualidade de Segurança**: Serviços independentes da manipulação de incidentes e tradicionalmente realizados por outras áreas da organização como: TI, Auditoria, Análise de Riscos, Avaliação de Produtos, Treinamentos, etc.

Resposta ao incidente é uma das funções desempenhadas no tratamento do incidente, que representa um dos serviços fornecidos como parte do gerenciamento de incidentes. A Figura 3 mostra a relação existente entre eles.

Figura 3 - Relação entre resposta, tratamento e gerenciamento de incidentes



Fonte: ALBERTS et al., 2004

2.3.4 Tarefas para o Tratamento de Incidentes

A definição das tarefas a serem realizadas durante as atividades de tratamento de incidentes irá contribuir na identificação das habilidades e ferramentas para realização do trabalho pela equipe do CSIRT (ALBERTS et al., 2004). A lista de tarefas utilizadas no tratamento de incidentes está descrita abaixo:

a) Sistemas de monitoramento e análise de *logs* da rede.
b) Análise de relatório para determinação de:
    a. Impacto;
    b. Escopo e abrangência;
    c. Sítios envolvidos;
    d. Metódos de ataque;
    e. Tendências em atividades de invasão.
c) Análise dos logs correspondentes e arquivos como:
    a. *Sniffer*, *firewall*, ou *logs* do roteador;
    b. Logs do UNIX ou *Windows*;
    c. Arquivos e ferramentas de invasão;
    d. Explorar *scripts*.
d) Pesquisa de sítios envolvidos ou informações de hosts para:
    a. Identificação do nome do *Host* / endereço IP;
    b. Determinar as informações de contato do *site*.
e) Contenção e eliminação das ameaças.
f) Prestação de assistência técnica direta:
    a. Assistência local;
    b. Resposta por email, telefone.

2.3.5 Ameaças no Ambiente

Com a evolução das máquinas e dos programas desenvolvidos com as tecnologias atuais, a questão da segurança também nos leva a refletir sobre os riscos e ameaças à segurança dos computadores, assim como os novos desafios que deverão ser enfrentados pela equipe de segurança nas organizações.

Operações comerciais e governamentais críticas são cada vez mais dependentes da internet para realização de suas atividades. O aumento da interação e interdependência

acontece devido à existência de clientes, parceiros, indústrias distribuídos no mundo globalizado. Não apenas a dependência da própria infraestrutura oferecida pelo uso da internet, assim como empresas de diversas áreas críticas como o transporte, aviação, telecomunicações, energia, serviços de emergência, dentre outros (ALBERTS et al., 2004). De acordo com Centro de Estudos, Resposta e Tratamento de Incidentes de Seguranca no Brasil (2012) muitas organizações ao acessarem a Internet estão sujeitas aos mais variados tipos de ataques, dentre eles estão a exploração de vulnerabilidades, varredura em redes (Scan), falsificação de *e-mail* (E-mail *spoofing*), interceptação de tráfego (*Sniffing*), força bruta (*Brute force*), desfiguração de página (*Defacement*), negação de serviço (DoS e DDoS), dentre outros.

2.3.6 Riscos e Segurança na Internet

Com a revolução da forma de realização dos negócios na internet, os riscos agregados à sua utilização podem ser fatais para organizações desprotegidas. Dentre eles podem ser citados: ataques à rede coorporativa, roubo de identidade, perda de informações sensíveis, adulteração de registros médicos, perdas financeiras, extorção para evitar a interrupção total do serviço, exposição de informações confidenciais, dentre outros. Há um grande número de vulnerabilidades de segurança em sistemas e aplicações disponíveis na internet. Muitas destas vulnerabilidades são exploradas porque a segurança não era a principal consideração no projeto dos protocolos de internet. O objetivo inicial da criação da internet era o compartilhamento de informações e recursos e não se pensava em controles de restrição e segurança.

Além disso, a complexidade e administração de infraestruturas de redes de computadores torna ainda mais difícil o gerenciamento adequado da segurança e dos recursos na rede. Como resultado, há muito mais ocorrência de incidentes, sem falar no fato dos administradores de redes não possuírem pessoas com capacitação adequada para implementar controles eficientes contra ataques e minimizar os danos (ALBERTS et al., 2004).

2.3.7 Ameaças e Vulnerabilidades Futuras

O que a comunidade da internet irá enfrentar em termos de segurança nos próximos anos, pode ser resumidos nos seguintes tópicos:

a) Aumento do número de empresas e usuários da internet;
b) Redução do desenvolvimento de produtos de fornecedores e do ciclo de testes;
c) Aumento da complexidade dos protocolos e aplicações executadas em clientes e servidores ligados à internet;
d) Aumento da complexidade da internet como uma rede;
e) Problemas no projeto de segurança da Infraestrutura de informação que não podem ser rapidamente resolvidos;
f) Aumento das habilidades e conhecimentos dos atacantes;
g) Aumento da sofisticação dos ataques de intrusão e ferramentas;
h) Aumento do número de invasões de computadores.

Em meados de 2006, percebeu-se que os ataques não eram aleatórios, mas objetivos. O motivo naquela época era a obtenção de dinheiro. Crimes Cibernéticos e o envolvimento de profissionais criminosos foram aumentando e consequentemente, aumentando também o número de violações de informações. Na utilização de técnicas de engenharia social, invasores enganavam suas vítimas nas relações de confiança para obtenção de informações pessoais.

As atividades de códigos maliciosos se tornaram um negócio com a compra e venda de ferramentas e kits. Agora, com o desenvolvimento de novas tecnologias, aparecem também novos ambientes que necessitam de proteção como as plataformas móveis, mundos virtuais, jogos online, redes sociais, computação na nuvem, dentre outros. Com o aperfeiçoamento das ferramentas de análise de vulnerabilidades foi possível aumentar o número de identificação de vulnerabilidades na rede (ALBERTS et al., 2004).

2.4 TRATAMENTO DE INCIDENTES DE SEGURANÇA

Neste tópico serão discutidos alguns conceitos relacionados à eventos de segurança em computadores, gestão de avaliação e o gerenciamento de incidentes adotado pelo CSIRTs.

2.4.1 Eventos de Segurança

O termo evento de segurança em computador refere-se às ocorrências em um sistema computacional ou até mesmo na rede que conecta este sistema ao mundo externo, sendo relevante para a segurança corporativa. Dentre os tipos de eventos que podem ser encontrados

neste cenário, incluem: qualquer ato de violação de política de segurança de forma explícita ou implícita; um conjunto de dados que representa um ou mais ataques relacionados; um evento adverso em um sistema e/ou rede de informações; e uma violação ou ameaça à violação das políticas de segurança corporativa.

2.4.2 Gestão de Avaliação

Para avaliar incidentes conforme orientações do CSIRTs, deve-se inicialmente utilizar técnicas de análise e soluções, considerando os conhecimentos organizacionais e de gestão envolvidos, para se obter uma avaliação eficaz. Dentro da organização é necessário fazer um levantamento de quais dados críticos e serviços precisam ser protegidos. Além disso, saber como é a interface de comunicação entre eles e com os demais. A velocidade com que uma organização reconheça, analise e responda a um incidente limitará os danos causados e consequentemente, poderá reduzir o custo de recuperação.

Mesmo tendo a melhor infraestrutura de segurança da informação, uma empresa não pode garantir que invasões ou outros atos maliciosos não aconteçam. Quando ocorrem incidentes de informação ou de tecnologia, será essencial que a organização apresente uma forma eficaz de resposta que permita um maior nível de resiliência operacional.

2.4.3 Gerenciamento de Incidentes

O termo gerenciamento de incidentes pode ser definido como a capacidade de fornecer gerenciamento fim a fim para eventos e incidentes que afetem diretamente os ativos de informação e tecnologia, dentro da organização. Para que uma organização apresente estratégias de resposta eficaz para proteger seus ativos críticos e infra-estrutura, o CSIRTs adota uma abordagem envolvendo várias camadas (áreas) de defesa, como as listadas abaixo:

a) Proteção da internet de riscos e ameaças internas;
b) Identificação da localização dos principais ativos e dados sensíveis;
c) Realização e avaliação de riscos;
d) Manter-se atualizado com as últimas versões de produtos e sistemas operacionais;
e) Instalar perímetros de defesa interna como: Roteadores, *Firewalls, Scanners* e monitoramento de rede e sistemas de análise;

f) Atualizar e difundir a tecnologia da informação e os procedimentos das políticas de segurança;
g) Fornecer treinamento de conscientização de segurança para os funcionários;
h) Formalizar um processo de gerenciamento de incidentes.

Gerenciamento de incidentes não é apenas a aplicação da tecnologia para resolver os eventos de segurança do computador. Requer o desenvolvimento de um plano de ação, um conjunto de processos na área que sejam consistentes e repetíveis, mensuráveis e compreendidos em toda a organização.

Neste capítulo foram apresentados os conceitos que envolvem o tema cibernética incluindo aspectos de segurança para o entendimento e tratamento de ameaças cibernéticas. O próximo capítulo define produto mecatrônico e apresenta os desafios no desenvolvimento de um projeto mecatrônico.

2.5 PRINCÍPIOS DE MECATRÔNICA

Neste capítulo serão discutidos alguns conceitos relacionados à mecatrônica, projeto de sistemas mecatrônicos, sistemas de controle e automação inteligentes, produtos mecatrônicos, abordando ainda os desafios de projeto em produtos mecatrônicos.

2.5.1 Definição de mecatrônica

O termo mecatrônica foi utilizado pela primeira vez no Japão, já no final da década de 70, como resultado do sucesso da combinação entre a mecânica, eletrônica e processamento digital em produtos de consumo. A integração desses conceitos possibilitou uma gama de desenvolvimento de aplicações, dando ao termo “mecatrônica” diferentes interpretações, dependendo da aplicação (ROSÁRIO, 2005).

Ashley (1997) define mecatrônica como sendo a integração de conhecimentos nas áreas de mecânica, elétrica e computação. Já Furukawa e Adamowski (2001) definem mecatrônica como uma combinação adequada de materiais (resistência dos materiais, comportamento térmico, etc.), mecanismos (cinemática, dinâmica), sensores, atuadores, eletrônica e processamento digital (controle, processamento de sinais, simulação, projeto auxiliado por computador). Esses autores definem ainda que a mecatrônica deverá possibilitar algumas características no projeto e no produto, sendo que, no projeto, deverá existir uma

simplificação do sistema mecânico e redução de tempo/custo de desenvolvimento; já no produto deverá incluir a flexibilidade de operação, inteligência, autodiagnóstico, precisão e confiabilidade.

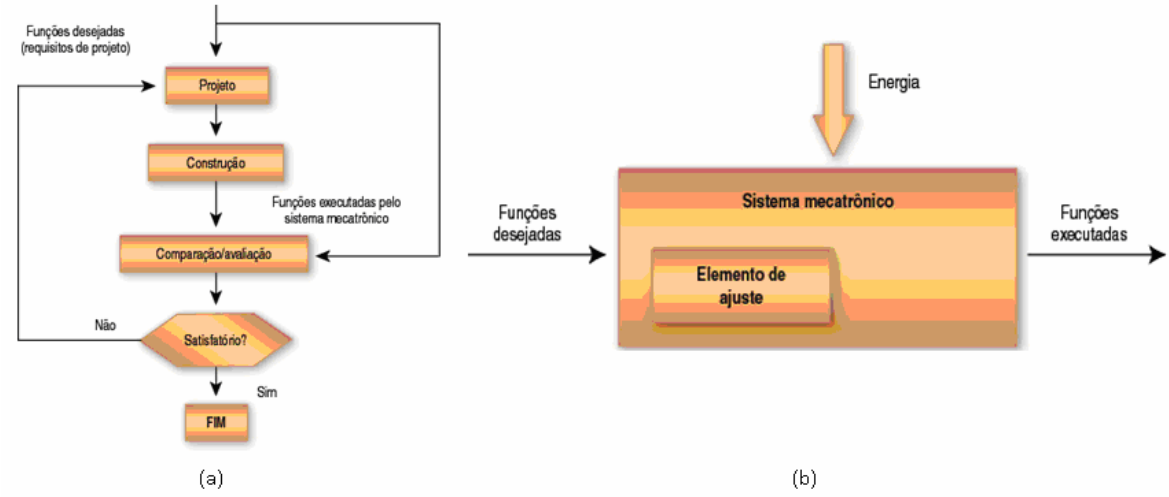
O termo mecatrônica é definido por Hunt (1998), como “uma abordagem multidisciplinar e integrada para o projeto de produtos e sistemas de manufatura”. O autor enfatiza ainda a importância da utilização de times multidisciplinares no projeto de produtos mecatrônicos, dando ênfase também ao aspecto integrador de tecnologias de grupo como: *computer aided process planning* (CAPP), *computer aided engineering* (CAE), *computer aided design* (CAD), *computer aided manufacturing* (CAM) e robôs, todos como impulsionadores da integração entre os diferentes grupos funcionais envolvidos no projeto de novos produtos.

Buur e Andreasen (1990) definem mecatrônica como uma tecnologia que combina mecânica com eletrônica e tecnologia da informação para compor tanto uma interação funcional como uma integração espacial de componentes, múdulos, produtos e sistemas. Segundo Rosário (2005), os projetos na área de robótica impulsionaram o desenvolvimento de outras áreas como o controle realimentado, tecnologias de sensores e atuadores, programação de alto nível, cinemática e dinâmica.

2.5.2 Sistemas Passivos e Ativos

O projeto de um sistema mecânico passivo e ativo é baseado nos princípios das ciências mecânicas, onde o projeto passivo deverá atender às necessidades tanto no aspecto geométrico do sistema e seus componentes quanto ao material utilizado em cada um deles (BARBALHO et al., 2014). Em um projeto de sistema mecânico passivo o projetista utiliza de conhecimentos diversos da engenharia como cinemática, dinâmica, resistência dos materiais, processos de criação, para definir a forma e a maneira de fabricação do sistema mecânico (ROSÁRIO, 2005). Já em um sistema mecânico ativo é realizada a inclusão do conceito de “controle automático”. Esse elemento de ajuste irá realizar correções de parâmetros internos do sistema para que se possa obter o resultado desejado, pois neste tipo de sistema as funções não são fixas, podendo variar. O conceito de controle automático é abordado por vários autores como em Kuo (1982), onde o elemento de ajuste atua sem a intervenção humana.

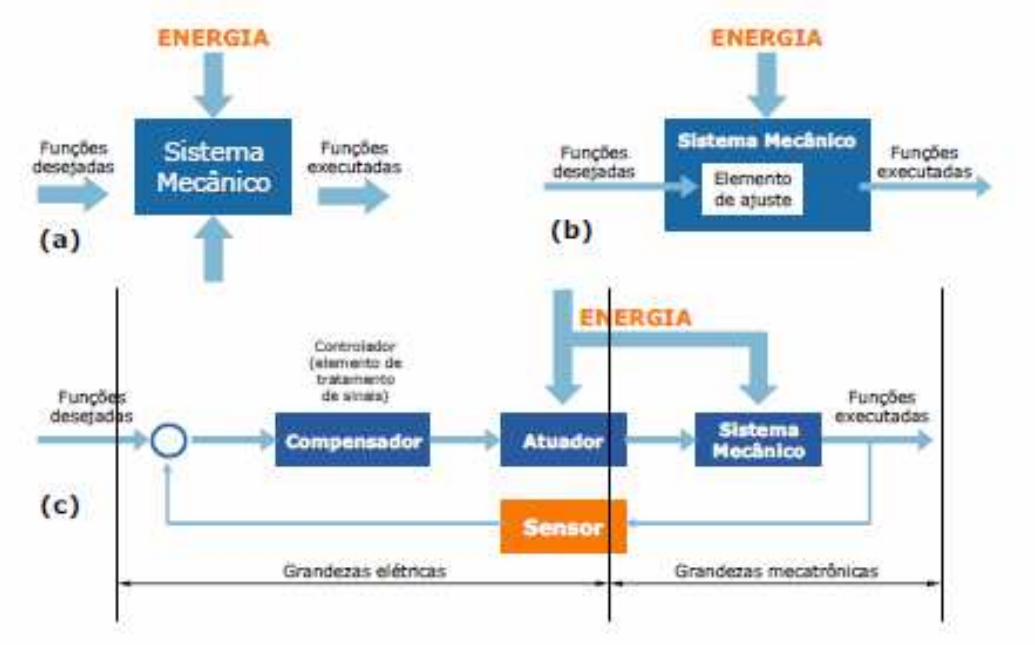
Figura 4 - Sistema mecânico (a) passivo e (b) ativo



Fonte: ROSÁRIO, 2005.

Horikawa (2000) define a mecatrônica como sendo um sistema mecânico com realimentação elétrica, classificando os projetos mecânicos como convencionais (passivos ou ativos) e mecatrônicos, conforme Figura 5 abaixo.

Figura 5 - Projetos mecânicos: (a) passivo; (b) ativo e (c) mecatrônico



Fonte: HORIKAWA, 2000.

Segundo o autor, projetos mecânicos conhecidos como passivos e ativos são completamente baseados em princípios físicos das “ciências mecânicas”. O processo de adaptação do produto no caso dos projetos passivos a uma nova necessidade é totalmente dependente da ação humana. Já em projetos ativos considera o conceito de controle através da

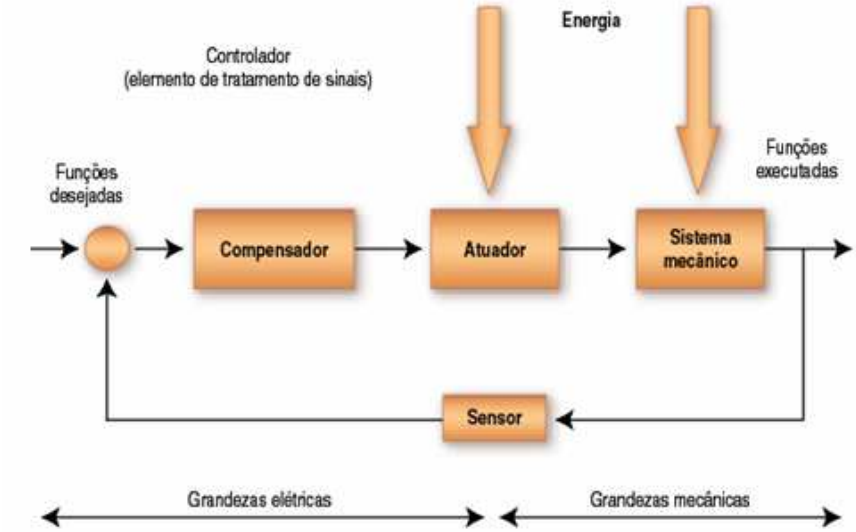
chamada malha de realimentação que é baseada em princípios mecânicos, a qual introduz elementos para ajuste e correções de parâmetros internos do sistema.

Dentre as limitações do controle por realimentação baseada em princípios mecânicos estão: (1) precisão no monitoramento do processo, (2) precisão no tratamento do sinal de controle, (3) complexidade do projeto, fabricação e montagem da malha de realimentação. Os sistemas mecatrônicos permitiram o aumento da precisão do controle dos parâmetros do projeto, além de maior rapidez no tempo de resposta e aumento na capacidade de implementação de algoritmos de controle mais complexos.

2.5.3 Sistemas Mecatrônicos

Em um sistema mecatrônico existe uma separação entre a parte do sistema que envolve as grandezas mecânicas das elétricas, sendo o controle automático realizado através da manipulação de informações, que no caso dos sistemas mecatrônicos acontece através de meios elétricos. A Figura 6 mostra a estrutura de um sistema mecatrônico:

Figura 6 - Estrutura de um sistema mecatrônico



Fonte: ROSÁRIO, 2005

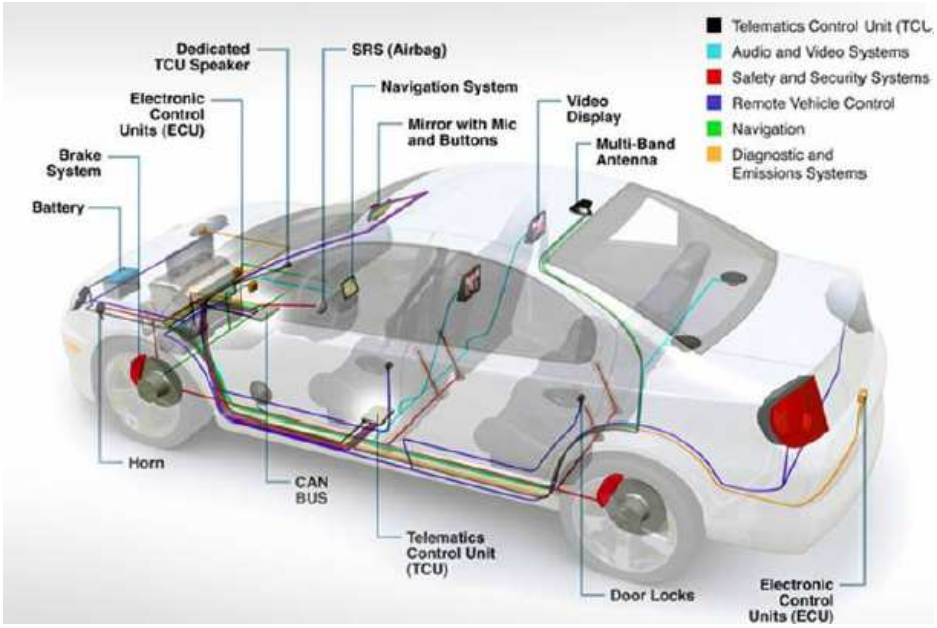
A mecatrônica apresenta algumas fragilidades por não conseguir explicar a existência de produtos típicos mecatrônicos, como os aparelhos DVD, CD-Player, periféricos da indústria de computadores, dentre outros. Ademais, a perspectiva da mecatrônica com base na engenharia mecânica não seria capaz de demonstrar as evoluções em equipamentos tipicamente eletrônicos. Apesar das limitações mecânicas, a compreensão da mecatrônica

como aplicação da eletrônica na área de engenharia mecânica pode esclarecer um número relevante de aplicações da mecatrônica (BARBALHO et. al., 2014).

A indústria automobilística é um grande exemplo dessas aplicações, como por exemplo, a presença dos sistemas eletrônicos embarcados. A eletrônica automotiva simplificou a fabricação de componentes, assim como a montagem de veículos pelas montadoras. Através do avanço da tecnologia existe cada vez mais a fusão entre componentes eletrônicos e os mecânicos/mecatrônicos tradicionais que possibilitarão no futuro uma montagem mais eficiente e segura (ANJOS, 2011).

Um sistema eletrônico embarcado utiliza processadores centrais para controle dos módulos distribuídos pelo veículo como por exemplo os microcontroladores e os processadores digitais de sinais. A presença de sistemas embarcados engloba desde os veículos elétricos e híbridos a freios inteligentes (*Anti-Lock Braking System* - ABS), controle de estabilidade (*Electronic Stability Control* – ESC/ESP), controle de tração (*Traction Control* - TCS), controle de telemática (*Telematic Control Unit* - TCU), dentre outros (ANJOS, 2011). A Figura 7 mostra o sistema de telemática de um veículo, o qual comanda os sinais necessários para executar as tarefas de telemática através da rede (CAN – *Controller Area Network*).

Figura 7- Sistema de telemática de um veículo



Fonte: BHATTI, 2009

2.5.4 Projeto de Sistemas Mecatrônicos

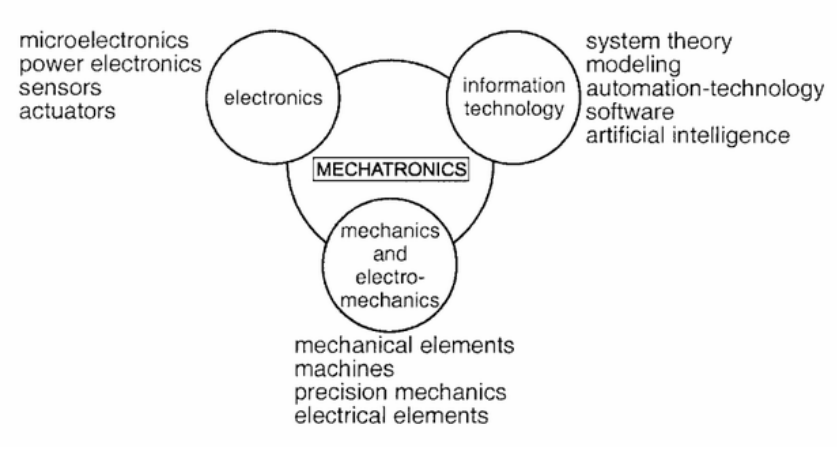
Segundo Rosário (2005) a metodologia de projeto para sistemas mecatrônicos deverá ser baseada nos seguintes itens:

a) Será possível a identificação entre a parte que trata do projeto mecânico e a que trata do projeto de controle;
b) A especificação do sistema ocorrerá diante da execução simultânea do projeto mecânico e do projeto de controle;
c) Em casos em que o projeto inicial não atenda às especificações iniciais, haverá duas alternativas para um reprojeto;
d) Será gerada especificação referente aos sensores, aos atuadores e à estratégia de controle.

Dessa forma, é possível que um projeto de um sistema mecatrônico planeje seus dispositivos e equipamentos com novas capacidades funcionais, mais precisas no atendimento às necessidades, e que apresente ainda a capacidade de suprir deficiências do projeto mecânico através do controle. Essas deficiências podem decorrer por exemplo, da dificuldade em se obter o modelo matemático que permita conhecer o comportamento mecânico de um dispositivo. A união da tecnologia mecânica com a de controle podem gerar dispositivos com melhor desempenho, que não seria obtido em projetos considerando apenas a parte mecânica (ROSÁRIO, 2005).

Por ser um campo interdisciplinar, a mecatrônica apresenta interação de diversas áreas como a mecânica, eletrônica, eletromecânica, de tecnologia, conforme exibido na Figura 8. Os produtos desenvolvidos em um projeto mecatrônico devem ser mais eficientes e mais econômicos quando comparados à abordagem tradicional, devido a uma maior flexibilidade, inteligência e confiabilidade apresentada por esses produtos, que possibilitam ainda uma redução no consumo de energia.

Figura 8- Mecatrônica: Integração de diferentes disciplinas

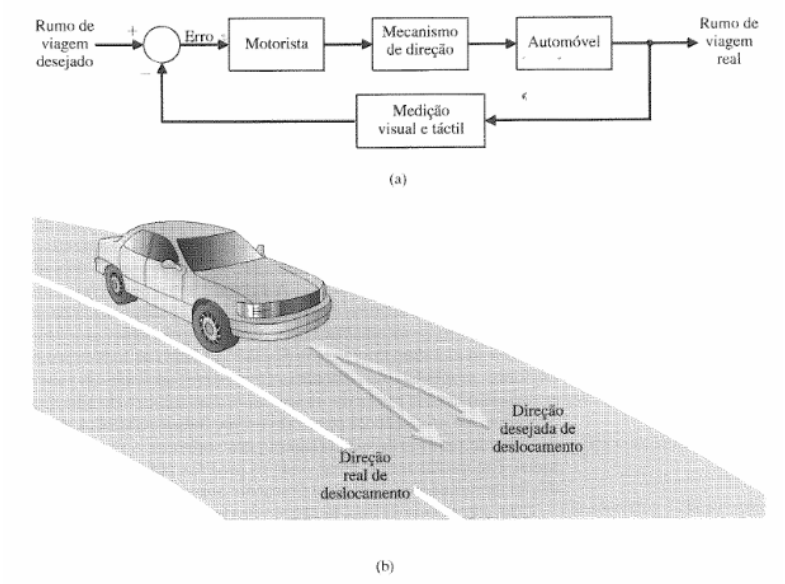


Fonte: ISERMANN, 2005

2.5.5 Sistemas de Controle e Automação Inteligentes

Na busca em oferecer produtos cada vez mais confiáveis e precisos a indústria automobilística tem usado do conceito de sistemas de controle no desempenho dos automóveis. Os sitemas de controle são utilizados para obtenção de aumento de produtividade e melhoria no desempenho de um produto ou serviço. A Figura 9 mostra um diagrama de blocos simples do sistema de controle de direção de um automóvel. A direção desejada é comparada com uma medida da direção real, para geração da medida de erro (DORF; BISHOP, 2001).

Figura 9 - Diagrama de blocos do sistema de controle de uma automóvel (a) e direção de deslocamento (b)



Fonte: DORF; BISHOP, 2001.

Os sistemas de controle do automóvel operam em malha fechada, onde a diferença entre a saída desejada e a saída real é igual ao erro, que é ajustado pelo dispositivo de controle, ou seja, “sinais de realimentação”. Já os sistemas que operam em malha aberta utilizam dispositivos atuadores para controlar o processo diretamente, sem o uso da “realimentação” (DORF; BISHOP, 2001).

Alguns sistemas de controle e automação inteligentes podem ser encontrados nos Cadernos Temáticos da Agência Brasileira de Desenvolvimento Industrial (2010), como os CLPs (Controladores Lógicos Programáveis), PACs (Controladores Programáveis para Automação), os quais utilizam tecnologias inteligentes como a inteligência artificial, lógica *fuzzy*, redes neurais e algoritmos genéticos para automação industrial. As organizações americanas *Advanced Manufacturing Research* (AMR), de Boston, e o *Gartner Group*, de *Stanford*, classificam os sistemas de gestão da produção em níveis de 0 a 3, conforme descrição abaixo:

a) Nível 0 ou de Controle: incluem os sitemas de controle industrial com *software* específico. Destacam-se neste nível os CLPs, SDCD (sistema digital de controle distribuído), comandos numéricos, robôs industriais, sistemas de supervisão e controle, dentre outros.
b) Nível 1 ou de Gerenciamento: incluem as funções de *software* responsáveis pela parte de gerenciamento do processo produtivo, integrando o nível de controle com o de planejamento. Este nível é chamado MES - *Manufacturing Execution Systems*.
c) Nível 2 ou de Planejamento: neste nível encontram-se as funções de planejamento de recursos e de materiais.
d) Nível 3 ou Corporativo: nível responsável pela integração de toda a empresa e fornecimento de suporte às decisões estratégicas.

A integração dos Sistemas de Informações de Manufatura com os Sistemas de Controle do Chão de Fábrica são integrados através dos MES (*Manufacturing Execution Systems*), provendo informações relativas ao processo produtivo que possibilita os sistemas de informações a formulação das estratégias de produção e de estoque. Tais informações são posteriormente conduzidas aos controladores de processos sobre eventuais mudanças nos processos de fabricação.

2.5.6 Produtos Mecatrônicos

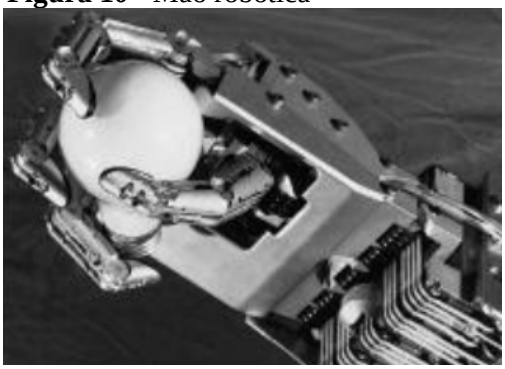
Segundo Bradley (1991), os produtos mecatrônicos devem apresentar alguns componentes como os descritos abaixo:

a) Sensores e instrumentação: componentes utilizados no produto para realizar controle de condições de operação. Podem ser acompanhados de transdutores que permitem a conversão de um tipo de energia em outro de melhor processamento pelo sistema.
b) *Software* de processamento/controle: considerado o principal componente lógico do sistema, permite armazenar e comandar as principais funções do produto. Em casos de requisitar alta confiabilidade e robustez do sistema de controle poderá ser substituído por projeto de lógica digital discreta ou através de *Field programmable gate array* (FPGA).
c) Atuadores e *drives*: componentes utilizados para correção do funcionamento do sistema. Geralmente são soluções mecânicas ou eletromecânicas que agem direto no mecanismo que executa a operação básica do produto. Já os *drives* são circuitos eletrônicos responsáveis pela interface com os sinais de controle, concedendo-lhes a potência essencial à alimentação dos atuadores.
d) Projeto de engenharia: caracteriza-se por ser o projeto elementar do mecanismo para o propósito ao qual o produto deverá atender. Quando integrado em sistemas mecatrônicos deverá considerar os demais componentes presentes.
e) Sistema de comunicação: esses sistemas não necessariamente estarão presentes em todos os produtos mecatrônicos. Sendo essenciais em projetos de sistemas de controle distribuído, como por exemplo em robôs de exploração interplanetária, aparelhos celular, dentre outros. Entre os meios de comunicação mais encontrados estão as redes locais (*Local Area Networks* - *LANs*) e os sistemas sem fio (*Wireless Fidelity* - WiFi).

Os robôs utilizados na indústria são um grande exemplo de produtos mecatrônicos e segundo Agência Brasileira de Desenvolvimento Industrial (2009) diferenciam-se de um dispositivo automatizado programável por apresentar capacidade de interatividade com o ambiente através de sensores, tomar decisões, capacidade de aprendizagem, realizar o

posicionamento correto através de movimentos de rotação/translação, dentre outras. Pesquisas realizadas pela Sociedade Brasileira de Comando Numérico - SOBRACON mostram que 60% dos robôs no Brasil realizam atividades ligadas à indústria automobilística (CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS, 2009). Número considerado ainda baixo quando comparado ao contexto mundial. Dentre as aplicações da robótica na indústria estão a soldagem por resistência por pontos (33%), manipulação de materiais (25%), soldagem por arco (18%), pintura (10%), dentre outras. A mão robótica exibida na Figura 10, possui 18 graus de liberdade e foi desenvolvida como ferramenta de pesquisa pelo *Center for Engineering Design* e pelo *Massachusetts Institute of Technology* MIT, sendo a mesma controlada por 5 microprocessadores motorola 68000 e acionada através de 36 atuadores eletropneumáticos de alto desempenho por meio de tendões polimétricos de alta resistência. Essa mão robótica utiliza sinais de realimentação de força, sendo controlada por sinais de controle bioelétricos do membro amputado, chamados sinais eletromiográficos. Possui 3 dedos e um polegar, bem como utiliza sensores de tato e tendões para o controle (DORF; BISHOP, 2001).

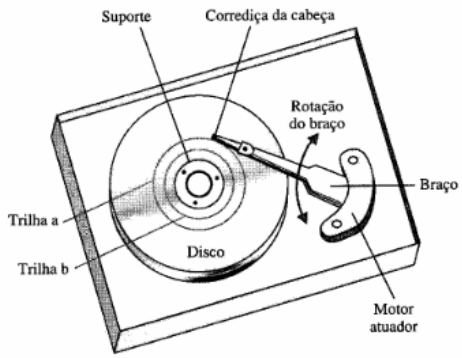
Figura 10 - Mão robótica



Fonte: (DORF; BISHOP, 2001)

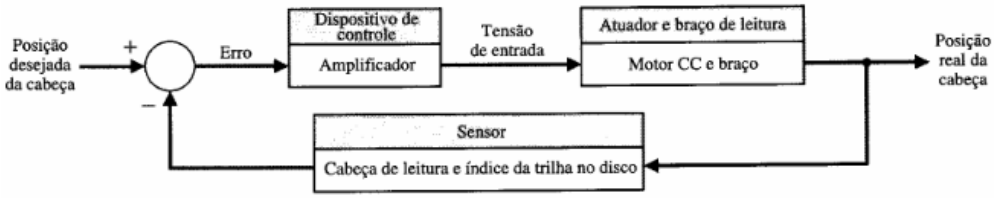
O periférico HD (*Hard Disk*) utilizado em computadores pode ser considerado um produto mecatrônico, devido à presença de alguns itens como o motor de rotação, responsável por manter uma rotação constante do mesmo. Além da presença das cabeças de leitura eletromagnéticas presas ao braço móvel, utilizadas para leitura e gravação de dados no disco. Os acionadores de disco, segundo Dorf e Bishop (2001), utilizados nos computadores representam uma aplicação da engenharia de controle.

Figura 11 - Acionador de disco



Fonte: DORF; BISHOP , 2001

Figura 12 - Diagrama de blocos do sistema de leitura do acionador de disco



Fonte: DORF; BISHOP , 2001.

2.5.7 Desafios de Projeto Mecatrônico

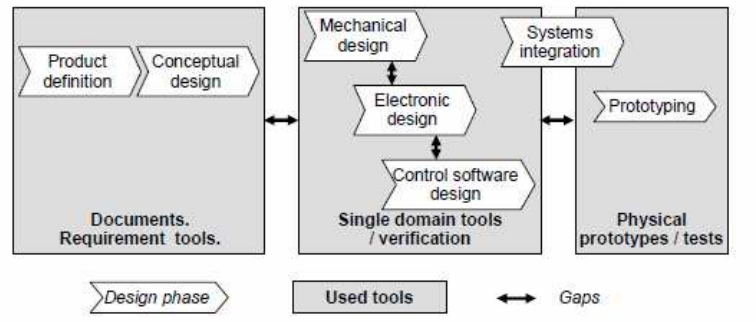
Em Cabrera et al. (2010) são apresentadas algumas abordagens para o desenvolvimento de produtos mecatrônicos baseadas em integração interoperável. Dentre elas está a plataforma baseada no conhecimento "*Design and Engineering Engine*", independente de área. Uma outra abordagem é o mecanismo de metamodelo de KIEF, onde são relacionados conceitos do sistema desde os atributos aos fenômenos físicos, onde o núcelo de KIEF representa uma base de conhecimento em que os objetos de diferentes ferramentas de modelagem podem ser mapeados uns aos outros através de fenômenos físicos, como pontos de conexão.

O trabalho de Cabrera et al. (2010) apresenta os desafios de desenvolvimento de um projeto para um produto mecatrônico, dentre eles a necessidade de integração do projeto devido ao grande número de funcionalidades apresentadas por um sistema mecatrônico, bem como a necessidade de ferramentas de integração apropriadas para tratamento de informações à nível de requisitos do sistema e acompanhamento das mudanças ao longo do projeto. Para tratar dos desafios de desenvolvimento de um projeto para produtos mecatrônicos os autores

propõem a criação de um *framework* para apoio à projetos integrados de sistemas mecatrônicos, abordando o desenvolvimento e controle de *software*.

A representação atual de um projeto mecatrônico, não contempla a utilização de ferramentas integradas que possam suportar as diversas áreas existentes no mesmo. As ferramentas atuais são específicas para áreas como a mecânica, controle, *software* e eletrônica. Conforme é exibida da Figura 13 cada fase possui seu próprio conjunto de ferramentas. As equipes de projeto são separadas por áreas de espcialização e muitas vezes nem se comunicam com as demais. Outro ponto a ser considerado é o fato da fase de integração ser adiada até o momento em que os protótipos físicos estejam disponíveis, gerando problemas de integração, pois partes do projeto de uma fase podem depender de outras.

Figura 13 - Representação atual do projeto mecatrônico



Fonte: CABRERA et al. , 2010.

O *framework* proposto no trabalho de Cabrera et al. (2010) é uma alternativa ao desenvolvimento de uma única ferramenta que englobe todas as informações do projeto, pois neste caso ela seria grande e complexa. Também há de se considerar que a realização de operações para modelar e lidar com diferentes tipos de dados do projeto em uma única ferramenta é um grande desafio.

2.6 DESENVOLVIMENTO DE PRODUTOS

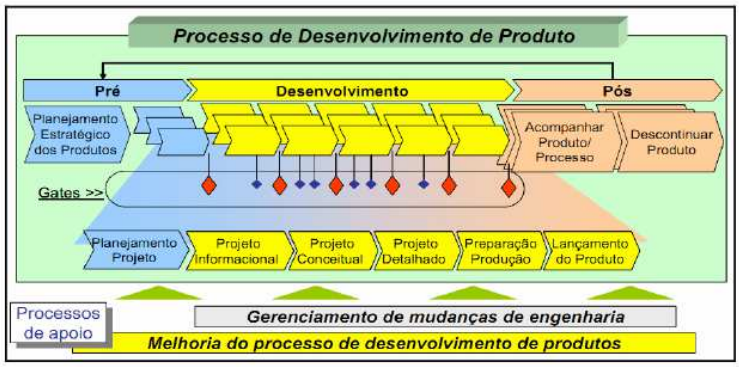
Neste capítulo serão discutidas as abordagens existentes para a compreensão do processo de desenvolvimento de produtos (PDP). Dentre elas, será apresentada a abordagem do modelo de referência mecatrônico de Barbalho (2006), a qual é a base para a proposta deste trabalho. Serão abordados os temas referentes às fases de homologação e validação do produto do referido modelo, que será utilizado para realizar estudos de casos em empresas fornecedoras de produtos cibernéticos.

2.6.1 Definição de Processo de Desenvolvimento de Produto

Em geral, o PDP consiste em um conjunto de atividades que são executadas na definição de novos produtos, incluindo a tomada de decisões, em que alternativas são identificadas e avaliadas com critérios previamente definidos. Sua função é integrar todos esses critérios e otimizá-los, considerando as restrições existentes de complexidade do produto, do processo de produção, de aspectos organizacionais e, também, de geração de custos com retrabalhos (CLARK; FUJIMOTO, 1991). A definição abrange todas as áreas de uma empresa, incluindo *marketing*, engenharia de produto e produção. Avalia o desempenho da mesma no desenvolvimento de produtos através dos seguintes parâmetros: qualidade, tempo e produtividade, os quais, conforme os autores devem ser otimizados visando o aumento da competitividade de seus produtos.

O processo de desenvolvimento de produtos proposto por Rozenfeld (2006) é voltado para empresas de manufatura de bens de consumo duráveis e de capital. O autor propõe uma divisão em três macrofases: Pré-desenvolvimento, Desenvolvimento e Pós-desenvolvimento, conforme apresentado na Figura 14.

Figura 14 - Processo de Desenvolvimento de Produto



Fonte: ROZENFELD, 2006

A primeira macrofase de Pré-desenvolvimento é composta pelas fases de planejamento estratégico do produto e planejamento do projeto. A macrofase de Desenvolvimento contempla as fases do projeto informacional, projeto conceitual, projeto detalhado, preparação para a produção e lançamento do produto. Após essa fase o modelo se encerra com a macrofase de Pós-desenvolvimento, onde é realizado o acompanhamento do produto por todo o ciclo de vida para sua posterior retirada do mercado. O modelo também adota um controle entre as fases (*gates)*, agindo como um ponto de revisão e aprovação formal do produto, para que então possa ser dado prosseguimento nas demais fases. Dessa forma, proporciona uma maior eficiência ao PDP, reduzindo falhas de processo.

Segundo Rozenfeld (2006), em seu capítulo de preparação da produção do produto, na certificação do produto podem ocorrer as seguintes atividades: avaliação das exigências de regulamentação, submissão ao cliente do processo de aprovação, avaliação dos serviços associados ao produto e obtenção da documentação para a certificação. O processo de certificação não acontece somente na fase de preparação da produção, podendo ocorrer desde a fase de projeto informacional. Caso seja exigida por órgão regulamentador a primeira certificação poderá ocorrer na fase de homologação do produto.

2.6.2 Abordagens de desenvolvimento de produtos

É possível encontrar diferentes abordagens para o desenvolvimento de produtos relacionados a diversas áreas da engenharia como por exemplo, mecatrônica, *software*, produção, dentre outras. No trabalho de Lonchanpt (et al., 2006) é apresentada uma proposta para descrever o projeto do processo de engenharia como um modelo evolutivo. Este modelo inicia-se com modelos genéricos onde posteriormente são detalhadas as representações existentes. Considera-se inicialmente o aspecto global da engenharia simultânea e posteriormente as atividades.

Um dos modelos mais consagrados do projeto deste processo é a abordagem sistemática de Pahl et al. (1996) onde considera-se o projeto do processo como um conjunto de fases sucessivas, sendo a primeira chamada de planejamento do produto e definição das tarefas, que consiste na análise e decomposição do problema do projeto e as etapas seguintes tratam da definição da solução. Estes estágios visam resolver o problema conforme uma progressão genérica, a partir dos aspectos mais globais para os mais detalhados.

O desenvolvimento de produtos pela abordagem sequencial faz com que o projeto obedeça uma sequência de fases, avançando de uma para outra somente após a conclusão da anterior. A adoção dessa abordagem segundo o trabalho de Cabrera et al. (2010), torna-se ineficaz, devido à ausência de um tratamento adequado entre as fases do projeto, trazendo um aumento de custo e tempo ao mesmo. Além disso, apresenta vários problemas para o desenvolvimento de produtos mecatrônicos, como as faltas de tratamento para as interdependências complexas entre os subsistemas existentes, de integração das ferramentas de análise de projeto utilizadas, de comunicação entre equipes e projetistas e de um ambiente para testes integrados, dentre outras.

Muitos destes problemas apresentados pela abordagem sequencial citada em Cabrera et al. (2010) podem ser minimizados pela adoção da abordagem simultânea ou paralela. Neste

tipo de abordagem consideram-se todas as fases do ciclo de vida do produto, desde a sua concepção até o seu descarte final. Cooper (1993) apresenta algumas vantagens da abordagem simultânea:

a) O processo de desenvolvimento de produtos torna-se mais intenso com muitas atividades sendo realizadas em um mesmo período de tempo, por diferentes pessoas;
b) Há uma chance menor de atividades ou tarefas falharem;
c) As atividades são executadas para encaixarem-se adequadamente umas às outras;
d) O PDP torna-se multifuncional e multidisciplinar, pois todo o time trabalha ao mesmo tempo, tomando parte nas revisões de fases e de projeto.

No trabalho de Chiochettam, Casagrande e Echeveste (2008) é realizada uma análise comparativa entre o modelo proposto por Rozenfeld (2006) e o processo de desenvolvimento de produtos de uma empresa do setor agrícola. A análise possibilita a identificação das fases que não foram adotadas pela empresa, colaborando na identificação de possíveis falhas em seu PDP, como por exemplo, a falta de definição de *gates* entre as fases, o que fragiliza o processo como um todo. Devido à introdução de novos produtos motivada pelo mercado, as empresas do setor siderúrgico devem dar a devida importância para a fase de preparação da produção, assim como apresentar um PDP estruturado, devido às suas características complexas (VARANDAS JUNIOR; MIGUEL, 2012).

2.7 MODELO DE REFERÊNCIA MECATRÔNICO

Neste capítulo serão discutidos alguns conceitos do Modelo de Referência Mecatrônico (MRM), definido por Barbalho (2006), apresenta-se a visão das atividades realizadas nas fases de homologação e validação do referido modelo, assim como a documentação gerada pelas mesmas.

A abordagem simultânea de Cooper (1993) se encaixa melhor no propósito deste trabalho, uma vez que possibilita o aumento do paralelismo entre as atividades de desenvolvimento, com destaque na realização simultânea das tarefas de projeto e planejamento de processo, Rozenfeld (2006). Existem outras abordagens para o desenvolvimento de produtos, como por exemplo, a definida por Barbalho (2006), como suporte ao desenvolvimento de produtos mecatrônicos, a qual foi escolhida uma vez que esses

produtos segundo Wiener (1984) são considerados essencialmente cibernéticos o que viabilizou sua utilização.

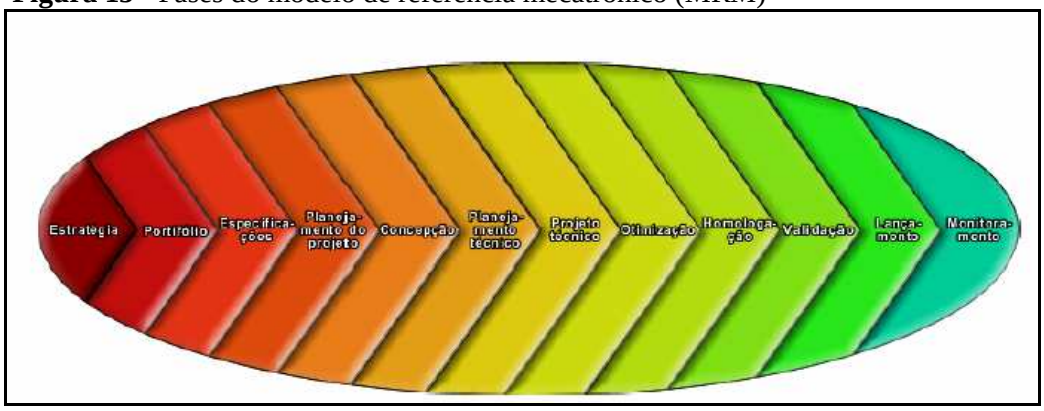
2.7.1 Modelo Lógico do MRM

O processo de desenvolvimento de produtos apresentado no MRM é composto por "fases" e "áreas de processo", sendo que nas fases ocorrem diversas atividades que mantém relação apenas com uma fase do desenvolvimento do produto. No caso das "áreas do processo", elas são compostas por várias "atividades", que por sua vez são compostas por tarefas, podendo apresentar relações com mais de uma "área de processo".

2.7.2 Modelo de Fases do MRM

As fases do MRM de Barbalho (2006) são baseadas na cadeia de agregação de valor, onde são definidas em função dos resultados. É composto por 12 fases: Estratégia, Portifólio, Especificações, Planejamento do projeto, Concepção, Planejamento técnico, Projeto técnico, Otimização, Homologação, Validação, Lançamento e Monitoramento. Através da Figura 15 pode-se visualizar a sequência das fases do referido modelo, descritas a seguir.

Figura 15 - Fases do modelo de referência mecatrônico (MRM)



Fonte: BARBALHO *et. al*. 2006, p. 106

a) Estratégia: São definidos os objetivos estratégicos a serem perseguidos em cada linha de produtos (LDP);
b) Portifólio: É definido o portifólio de cada LDP;
c) Especificações: Definem-se as especificações de cada produto;
d) Planejamento do Projeto: É realizada a definição do plano de projeto;

e) Concepção: São definidos os principais componentes e princípios de solução para as principais funções do produto mecatrônico;

f) Planejamento Técnico: É realizado o detalhamento do plano de projeto com base na concepção definida;

g) Projeto Técnico: São apresentadas soluções para as principais funções do produto;

h) Otimização: É realizado o detalhamento e teste de soluções para funções secundárias do produto, assim como a realização de análises necessárias para o aumento da robustez e confiabilidade do produto;

i) Homologação: É realizada a homologação do processo de fabricação e montagem do produto;

j) Validação: É realizada a validação e certificação do produto;

k) Lançamento: É realizado o lançamento do produto no mercado;

l) Monitoramento: É realizado o acompanhamento dos resultados adquiridos com o produto e o gerenciamento das modificações realizadas na configuração inicial de produção.

2.7.3 Tomada de Decisão do MRM

Ao término de cada fase do MRM de Barbalho (2006) é realizada uma tomada de decisão ao longo do PDP. As decisões das fases de homologação e validação consistem na atualização do plano de projeto do produto, com revisão das metas de custo tanto do projeto como do produto, além das previsões de venda. Decisões estas realizadas pela alta direção da empresa. Neste trabalho serão detalhadas apenas as fases de Homologação (9) e Validação (10) do referido modelo.

2.7.4 Fase de Homologação

Segundo o MRM de BARBALHO (2006) essa fase tem como propósito refinar o projeto do processo e comprovar que o produto final produzido em condições normais de operação nas linhas de produção corresponde às soluções técnicas desenvolvidas pela equipe de desenvolvimento. O projeto do processo de um produto mecatrônico integra soluções para as partes mecânicas, eletrônicas e de *software* desenvolvidas. Esse projeto consiste no detalhamento dos desenhos de fabricação e das folhas de processo das peças mecânicas, bem como no detalhamento dos *gerbers* e listas de montagem necessários à fabricação e à

montagem eletrônica e os procedimentos pelos quais o *software* deve ser integrado às soluções de *hardware*.

Esta fase é baseada na ideia de que é necessário realizar o detalhamento do processo de fabricação e montagem antes que sejam incluídos custos relacionados ao registro e certificação do produto. A entrada da fase de homologação do produto do modelo de Barbalho (2006) é a configuração do protótipo beta (protótipos completo do produto) aprovado na fase de otimização. De posse da *baseline* da configuração de projeto_2 serão realizadas as atividades descritas nos subitens 2.7.4.1 a 2.7.4.9.

2.7.4.1 Projeto da Embalagem

O projeto da embalagem do produto é de fundamental importância, apresentando soluções tecnológicas tais como o tipo do material a ser utilizado, questões ambientais e de *design*, funcionais, como a capacidade de armazenar informações acerca do manuseio e transporte ao qual o produto foi submetido, além das relacionadas com a proteção mecânica do produto embalado, dentre outras.

Ademais, é baseado no fluxo de projeto mecânico, uma vez que as soluções desenvolvidas são basicamente relacionadas com formas, dimensões, materiais e processos.

As atividades para projetar a embalagem, segundo Rozenfeld (2006), englobam: avaliar a distribuição do produto como o transporte e entrega, definir as formas e as sinalizações das embalagens do produto, como identificar os elementos críticos, adequá-la a esses elementos, além de projetar e planejar o seu processo.

Deve-se então consolidar os requisitos da embalagem do produto com base no seu *design*, nos aspectos normativos relacionados com a embalagem nos mercados onde será introduzido. O próximo passo é adequar os requisitos de embalagem em um projeto de *design* do produto que atenda às especificações relacionadas com ao seu conceito. Deve-se então realizar um *trade-off* entre requisitos de *design*, operações de manufatura e de logística necessárias ao produto.

O *trade-off* determinará a importância das decisões de projeto de embalagem a serem tomadas. A embalagem é então projetada considerando aspectos de projeto da engenharia básica do produto, e em determinadas situações, quando se fizer necessário, o projeto da eletrônica e do sistema de controle. Após o projeto da embalagem a próxima e última etapa é o planejamento dos processos de embalamento e desembalamento (BARBALHO, 2006).

2.7.4.2 Revisar e Documentar Instalação e Configuração de Software

Neste passo é realizado o detalhamento da documentação necessária ao carregamento e teste do *software* que será desenvolvido. Quando necessário, deve-se realizar a configuração do computador e/ou ajustes no *hardware*, visando ao adequado funcionamento do *software* e identificação de defeitos no *hardware.*

A documentação deverá permitir a realização de testes com o *software* desenvolvido, incluindo testes de monitoramento para verificação da conexão do *hardware* com outras partes do equipamento, assim como para a identificação de defeitos. Como saída para esta atividade há um procedimento detalhado de instalação e configuração de *software*, no qual constem os testes a serem realizados na integração do *software* ao *hardware* relacionado.

2.7.4.3 Revisar Documentação Mecânica

Esta atividade engloba o detalhamento das especificações necessárias à aquisição, fabricação e montagem de partes e componentes mecânicos do produto. As partes mecânicas que compõem o produto mecatrônico podem ser divididas em partes fabricadas e compradas, sendo as partes fabricadas a realização dos processos de fabricação mecânica sobre materiais metálicos ou não-metálicos adquiridos. As especificações são basicamente os materiais que serão processados e o detalhamento dos processos de fabricação a serem utilizados. Faz parte da especificação de montagem mecânica o detatalhamento dos desenhos de fabricação, incluindo também os componentes de cada submontagem do produto.

O detalhamento da documentação de fabricação e montagem mecânica inicia-se com a consolidação das listas de peças e componentes de cada parte, subsistema, e submontagem do produto. Deve-se utilizar a análise *Failure Mode and Effect Analysis* (FMEA), para se obter informações de possíveis peças críticas, materiais e processos de fabricação. A técnica FMEA foi utilizada também pela *Ford Company*, empresa automotiva que a adotou em seu conceito de garantia da qualidade (ROZENFELD, 2006). As saídas para esta atividade incluem listas de peças para montagem e de materiais para aquisição, folhas de processos e procedimentos de montagem mecânica.

2.7.4.4 Revisar Documentação Eletrônica

Esta atividade engloba o detalhamento da documentação de aquisição, fabricação, montagem e testes das partes eletrônicas do produto. Incluem as seguintes atividades: geração de listas de compra de componentes eletrônicos, de *gerbers* utilizados para a fabricação das placas eletrônicas, de especificações de ambiente de fabricação e montagem eletrônica, bem como detalhamento dos esquemáticos de cablagem e conexões, de listas e mapas de montagem e dos procedimentos de montagem eletrônica e revisão da documentação de teste da eletrônica.

2.7.4.5 Desenvolvimento de Recursos de Produção

Nesta atividade é incluído o projeto dos moldes e dispositivos necessários à fabricação do produto em escala comercial, incluindo também o projeto de ferramentas de fabricação e montagem, tais como de moldes de injeção plástica, estampos de corte, castanhas, grampos e dispositivos de fixação em geral, suportes de montagem, dispositivos especiais de crimpagem, dentre outros. A geração da documentação desta atividade incluem análise do processo de fabricação e montagem (mecânica e eletrônica) e detalhamento do projeto de moldes e dispositivos de fabricação e montagem.

Muitas empresas necessitam de recursos especiais para conseguir fabricar seus produtos, necessitando de procedimentos sistemáticos para uma boa escolha dos fornecedores, principalmente no apoio da assitência técnica, manutenções e melhoria do esquipamento, (ROZENFELD, 2006).

2.7.4.6 Procedimento de Instalação e Configuração de Software

Este procedimento descreve as atividades necessárias à instalação e configuração dos *softwares* utilizados no equipamento. Dentre elas estão a descrição das atividades necessárias à instalação do *software*, a referência à versão do *software* válida e as atividades necessárias à configuração do computador.

2.7.4.7 Documentação de Fabricação e Montagem (Mecânica e Eletrônica)

O procedimento desta documentação descreve as atividades necessárias à fabricação e montagem tanto mecânica como eletrônica do equipamento, que incluirão a especificação dos materiais e componentes mecânicos e eletrônicos a serem adquiridos, folhas de processo para cada peça a ser fabricada, incluindo as placas de circuito impresso (*gerbers*), descrição das atividades necessárias à montagem das partes mecânicas do equipamento e partes eletrônicas, assim como das atividades necessárias ao teste para montagens mecânicas e eletrônicas.

2.7.4.8 Análise de Custos e Falhas no Processo

As documentações geradas anteriormente são analisadas visando possibilidades de redução dos custos do produto a partir da análise do projeto baseada em técnicas de *Design for Manufacture and Assembly* (DFMA). Ulrich e Eppinger (1995) definem DFMA como uma metodologia altamente integrativa que exige contribuições de todos os membros do time de desenvolvimento, assim como de outros profissionais da empresa.

A empresa também deverá se preocupar com as falhas no processo, *Failure Mode and Effect Analysis* (FMEA) devendo ocorrer em paralelo à aplicação da técnica DFMA. Dessa forma, é possível que as alterações do projeto necessárias à redução dos custos sejam analisadas quanto ao seu impacto no risco de falhas do processo, antes mesmo que sejam determindas as ações de revisão do mesmo.

2.7.4.9 QAMT: Qualidade, Aquisições, Manufatura e Testes

A próxima etapa é analisar o desenvolvimento do controle de qualidade do processo produtivo com o desenvolvimento de planos de controle para os itens críticos de processo. Inicia-se com o detalhamento da documentação de aquisição, de forma a contribuir com o processo de homologação dos fornecedores. É realizada a aquisição, a fabricação dos moldes e dispositivos de fabricação, para serem posteriormente instalados e testados.

Os protótipos de homologação são fabricados e testados no mercado com a geração do relatório de homologação do processo que deverá conter dados relativos à capabilidade do processo de fabricação e montagem. Em setores onde os requisitos de qualidade são rígidos, os valores-meta “capabilidade de processo potencial” (Ppk) no qual são removidas as causas de variação potencial do projeto projetado e/ou “capabilidade de processo executado” (Cpk)

no qual os dados são coletados com todo o processo correndo em escala comercial e com todas as variações possíveis, são mais apertados, enquanto em outros setores de baixo volume o processo deverá ser orientado conforme definição de Crosby (1999) chamada por “zero defeito”, Barbalho (2006). O último passo é a verificação da qualidade dos resultados da fase e posteriormente a documentação pertinente, com a geração de uma nova configuração do projeto. A fase de validação do produto só é iniciada após a conclusão satisfatória dos resultados obtidos da fase de homologação.

2.7.5 Fase de Validação

Segundo o MRM de Barbalho (2006) essa fase apresenta dois propósitos básicos. A primeira pretende validar o produto com o cliente, ou seja, terá que estar em conformidade com a norma ISO 9001. A segunda deverá certificar o produto e garantir que seu funcionamento não apresenta riscos à segurança do usuário final. A validação do produto é uma atividade fundamental, pois é através dela que se demonstra que os produtos e seus componentes atendem ao seu propósito final quando utilizados em locais e condições de operação adequados. É também nesta atividade que os testes com os protótipos tipo ALFA, BETA e de homologação tiveram como fundamento a verificação das especificações do produto.

Os protótipos alfa têm como objetivo provar a efetividade das soluções desenvolvidas para as funções primárias do produto e são utilizados na fase de projeto técnico. Já o protótipo beta representa os protótipos completos do produto e são utilizados na fase de otimização, enquanto que os protótipos de homologação tem como propósito a validação do processo de fabricação, em condições normais de operação do produto. As atividades da fase de validação do produto do modelo de Barbalho (2006) são descritas nos subitens seguintes.

2.7.5.1 Planejamento da Validação e Certificação do Produto

O início do planejamento da validação e certificação do produto é a análise dos resultados dos testes de uso do mesmo. A partir deste ponto será decorrente o posicionamento final que o produto passará a ter frente aos seus concorrentes. A minuta do projeto deve ser refinada com a descrição do impacto do produto no portifólio da empresa. O produto deverá ser documentado em conformidade com as normas a ele aplicáveis.

Conforme o MRM de Barbalho (2006), faz parte desta atividade a geração dos seguintes itens: análise dos resultados de testes de uso do produto e posicionamento das especificações, refinamento da minuta do projeto quanto ao portifólio planejado, planejamento dos clientes e submissão do produto para validação, definição de marcas de qualidade certificada necessárias ao produto, planejamento dos locais e datas de certificação laboratorial e auditorias de qualidade.

2.7.5.2 Documentação do Produto

Nesta atividade deve-se incluir a documentação de uso do produto, tais como manuais de instruções, informações gerais de segurança e relatório técnico global. Essa documentação é necessária devido à exigência por órgãos certificadores para a análise de adequação normativa do produto, além da documentação indispensável à assistência técnica e aos documentos necessários ao seu uso por parte do cliente final.

2.7.5.3 Protótipos de Validação

Nesta atividade são incluídos os protótipos de validação que têm como objetivo comprovar que o produto desenvolvido, fabricado e montado pelo pessoal de linha em condições normais de operação, atende às necessidades do cliente e aos requisitos normativos aplicáveis. Inicialmente é realizada a identificação das partes do equipamento a serem substituídas, em função de eventuais alterações de projeto baseadas em requisitos normativos adicionais, necessários aos mercados nos quais o produto será introduzido. A partir deste ponto, são fabricados e montados os subsistemas a substituir e inspeções de processo. Ao final desta atividade é gerado um relatório de verificação do produto revisado.

2.7.5.4 Validação do Projeto

A atividade de validação do projeto envolve uma série de subatividades relacionadas aos testes, desde o seu planejamento até à documentação dos resultados finais. São realizados testes de aceitação do *software* projetado, sendo que a ideia é repetí-los com o intuito de sanar possíveis problemas relacionados ao uso do *software* em condições normais e extremas de operação, como por exemplo, os testes de performance de carga e *stress*.

Os resultados dos testes deverão ser documentados de forma a subsidiar a definição final de versões do produto a serem submetidas ao processo de certificação, assim como alterações necessárias ao projeto. O projeto é então validado com a geração do relatório de validação do produto, o qual contém informações pertinentes ao mesmo, como versões e resultados de testes realizados pelos clientes.

2.7.5.5 Revisão de versões e Modificações

São atividades extremamente importantes uma vez que a revisão de versões do produto permite classificar os resultados dos testes de validação com os diferentes clientes, visando à definição das diferentes versões que serão submetidas aos órgãos reguladores. Dessa forma, caso seja necessário a adequação do produto às alterações sugeridas pelos clientes, será realizada a atividade de modificações relacionadas às diferentes versões do produto.

2.7.5.6 Certificação do Produto

Certificação pode ser definida como um processo no qual uma terceira parte acreditada avalia se determinado produto atende às normas técnicas. Esta avaliação é .baseada em auditorias no processo produtivo, na coleta e em ensaios de amostras. Diferente dos laudos e relatórios de ensaios que servem para demonstrar que determinada amostra atende ou não uma norma técnica, a certificação serve para garantir que a produção é controlada e que os produtos estão atendendo às normas técnicas continuamente (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015). Conforme Barbalho (2006), uma vez revisado pela atividade anterior, é necessário submeter o produto a procedimentos de testes e de auditorias que permitam certificar o produto baseado em padrões internacionalmente reconhecidos. Os resultados desses testes podem demandar novas alterações no produto para adequação normativa. O próximo passo é a verificação da qualidade da validação do produto para posterior documentação, o que gera uma nova configuração do projeto. Essa documentação servirá como análise para possíveis melhorias dos procedimentos a serem seguidos, consequentemente melhorando a qualidade do PDP da empresa.

Propõe-se nesta dissertação a realização de um diagnóstico da sistemática de homologação e certificação de produtos cibernéticos através da comparação com o Modelo de Referência Mecatrônico (MRM), proposto por Barbalho (2006). Para isso serão apresentados às empresas do estudo de caso três formulários: Formulário de Análise do Processo de

Homologação do Produto (APÊNDICE A), Formulário de Análise do Processo de Certificação do Produto (APÊNDICE B) e Formulário de Análise baseado na Norma ISO/IEC_15408: *Common Criteria for Information Technology Security Evaluation* (APÊNDICE C).

Os requisitos para segurança de Produtos/Serviços de TI previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) podem ser encontrados no (APÊNDICE D) e incluem orientações para o desenvolvedor e auditor. Sua estrutura caracteriza-se pela hierarquia de (classes, famílias e componentes). O nível mais externo é a classe que é composta por famílias, e dependendo do nível de proteção escolhido *Evaluation Assurance Level* (EAL1 a EAL7), poderá incluir mais ou menos famílias, para garantir dessa forma, o objetivo do nível escolhido. Cada família por sua vez apresenta componentes para garantia da segurança do produto. Por exemplo, para o nível (EAL1) a classe "Desenvolvimento" apresenta apenas uma família: ADV_FSP.1 *Basic functional specification*; enquanto para o nível (EAL2) apresenta três famílias: ADV_ARC.1 *Security architecture description*, ADV_FSP.2 *Security-enforcing functional specification* e ADV_TDS.1 *Basic design* e assim por diante.

A Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) apresenta orientações tanto para consumidores, ao selecionar componentes para garantia dos requisitos de segurança; como para desenvolvedores ao aplicarem os requisitos no desenvolvimento do produto e auditores que utilizam desses requisitos como critérios de avaliação obrigatória.

3 METODOLOGIA

Neste capítulo será abordada a metodologia de pesquisa para realização do estudo proposto. No item 3.1 será apresentada a classificação da pesquisa quanto à natureza, aos objetivos gerais, aos procedimentos e à abordagem do problema e no item 3.2 será apresentado a definição de estudo de caso conforme literatura pertinente.

3.1 CLASSIFICAÇÃO DA PESQUISA

Segundo Gil (2010), para ser considerado um bom pesquisador, além do conhecimento do assunto, é preciso ter algumas características como a curiosidade, criatividade, integridade intelectual e sensibilidade social, sendo proporcionalmente essenciais a humildade, a imaginação disciplinada, a paciência e a confiança na experiência.

Pesquisa pode ser definida como

> atividade básica das ciências na sua indagação e descoberta da realidade. É uma atitude e uma prática teórica de constante busca que define um processo intrinsecamente inacabado e permanente. É uma atividade de aproximação sucessiva da realidade que nunca se esgota, fazendo uma combinação particular entre teoria e dados (MINAYO, 1994, p. 23).

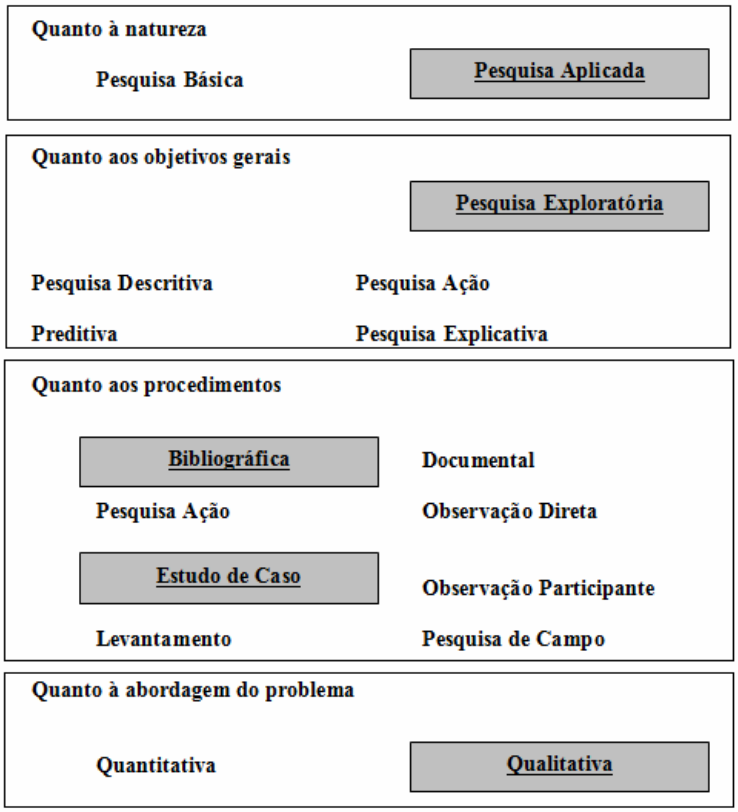
Segundo Demo (1996), pesquisa pode ser considerada uma forma de atitude, uma forma de questionamento sistemático, crítico e criativo, adicionado à intervenção competente na realidade, ou o diálogo crítico permanente com a realidade em sentido teórico e prático. Para Minayo (1994), pesquisa é considerada como uma atividade básica das ciências em sua indagação e descoberta da realidade, sendo composta de atitude e prática teórica de constante busca na definição de um processo intrinsecamente inacabado e permanente. É caracterizada por uma atividade de aproximação sucessiva da realidade que nunca se esgota, construindo uma combinação única entre teoria e dados. A Figura 16 apresenta a classificação da pesquisa utilizada neste trabalho quanto aos seguintes aspectos: natureza, objetivos gerais, procedimentos e abordagem do problema, sendo representados por caixas cinzas.

Quanto à natureza da pesquisa este estudo caracteriza-se pela pesquisa aplicada que trata da produção de conhecimento com aplicações práticas, sendo dirigida a soluções de problemas específicos. Envolve verdades e interesses locais. De acordo com Gil (2008, p. 27) “a pesquisa aplicada possui muitos pontos de contato com a pesquisa pura, pois depende de suas descobertas e se enriquece com o seu desenvolvimento”. Quanto aos objetivos gerais é possível classificar este estudo como pesquisa exploratória, segundo GIL (2008), pode

envolver levantamento bibliográfico, entrevistas com pessoas experientes no problema pesquisado. Geralmente assume a forma de pesquisa bibliográfica e estudo de caso. É exploratória principalmente pelo fato de ser um tema pouco explorado, com pouco bibliografia científica à respeito.

Os procedimentos utilizados neste estudo caracterizam-se pela pesquisa bibliográfica e estudo de caso. A pesquisa bibliográfica de acordo com GIL (2008) é desenvolvida com material já elaborado, constituído principalmente de livros e artigos científicos. Já o estudo de caso consiste em um estudo profundo e exaustivo de um ou poucos objetos, de forma que possibilite seu amplo e detalhado conhecimento.

Figura 16- Classificação da Pesquisa



Fonte: elaborado pelo autor

Sob os aspectos da abordagem do problema classificou-se este estudo como pesquisa qualitativa, a qual não é traduzida em números, pois pretende verificar a relação da realidade com o objeto de estudo, obtendo várias interpretações de uma análise indutiva por parte do pesquisador. Gil (2008) considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito

que não pode ser traduzido em números. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento chave para tal.

3.2 DEFINIÇÃO DE ESTUDO DE CASO

Conforme Gil (2008) o estudo de caso é um método de investigação em pesquisa social que apresenta as seguintes características: (1) Estudo de poucos objetos de pesquisa de maneira aprofundada; (2) Investigação de fenômenos e condições específicas e (3) Utilização favorável na análise de temas com alta complexidade, permitindo a formulação de problemas e construção de hipóteses.

Estudo de caso no conceito de Yin (2005) é uma investigação empírica que investiga um fenômeno contemporâneo dentro do contexto da vida real, sendo adequado quando as circunstâncias são complexas e podem sofrer mudanças, ou mesmo quando as condições não forem encontradas antes. Apresenta situações politizadas onde existem muitos interessados. A utilização do estudo de caso agrega alguns benefícios segundo vários autores. Miguel (2007) oferece o aumento da compreensão e do entendimento sobre os eventos reais contemporâneos. Eisenhardt (1989) inclui uma descrição que permite o teste de uma teoria existente, assim como o desenvolvimento de uma nova teoria.

Yin (2005) define o estudo de caso em quatro tipos: casos únicos, casos múltiplos, enfoque incorporado e enfoque holístico. O estudo de casos múltiplos conforme o autor é mais consistente por permitir maior generalização dos resultados. Sendo que a escolha do número de casos de uso não deve se basear na lógica da amostragem, e sim em uma decisão baseada no reflexo do número de replicações do caso desejadas pelo pesquisador em seu estudo.

Segundo o autor, em um estudo de caso é necessário que se utilize um protocolo para garantir a confiabilidade da pesquisa, servindo como orientação ao pesquisador na coleta de dados. Protocolo pode ser definido, conforme Martins (2008), como um conjunto de códigos, menções e procedimentos suficientes para se replicar o estudo de caso original e oferecer condições práticas para se testar a confiabilidade do estudo. Neste estudo será adotado o estudo de casos múltiplos, com a investigação através do diagnóstico da sistemática de homologação e certificação de produtos cibernéticos em empresas brasileiras que desenvolvam e/ou forneçam tais produtos.

4 DESENVOLVIMENTO DOS ESTUDOS DE CASOS

Este capítulo aborda os estudos de casos realizados na pesquisa em campo, utilizando dois tipos distintos: três órgãos públicos e duas empresas do setor privado instaladas em Brasília. As empresas privadas são fornecedoras de produtos cibernéticos, sendo a Empresa A desenvolvedora, porém a Empresa B não desenvolve, recebe o produto diretamente do fabricante e realiza os ajustes finais para entrega aos clientes. Os órgãos públicos pesquisados apresentam procedimentos específicos para a homologação e certificação de produtos cibernéticos desenvolvidos por empresas privadas.

No primeiro item, discute-se a seleção e apresentação das empresas/órgãos para o estudo em campo, caracterizando-as segundo o processo de homologação e certificação de produtos. No segundo item é apresentada uma descrição das atividades inerentes à coleta de dados das empresas privadas e posteriormente dos órgãos reguladores. Em seguida são apresentados e discutidos os resultados obtidos nos estudos de casos.

Definiu-se que as empresas privadas deveriam fornecer ou desenvolver produtos/serviços cibernéticos, os quais poderiam ser para atender ao setor público ou privado. No caso dos órgãos públicos deveriam apresentar procedimentos de homologação e certificação para produtos cibernéticos. A realização da pesquisa está diretamente relacionada à abertura e disponibilidade das empresas em prover documentos ou realizar entrevistas para o estudo.

Do universo de casos disponível para o pesquisador, caracterizado por empresas que fornecem ou desenvolvem produtos/serviços cibernéticos, no caso das empresas privadas, foram identificadas algumas de maior interesse, cujos produtos são submetidos ao processo de certificação, podendo ser utilizado para proteção em infraestruturas críticas ou que apresente características de proteção cibernética em casos de violação da segurança. No caso dos órgãos públicos, buscou-se, além dos procedimentos para homologação e certificação de produtos cibernéticos, requisitos para aquisição de produtos em conformidade com as necessidades da Administração Pública Federal; e em alguns casos com a contribuição na indicação de outros pesquisadores.

Considerando a necessidade adicional de ser realizada a pesquisa dentro do Distrito Federal, por questões de acesso, o pesquisador levantou uma possibilidade de realização da pesquisa em cerca de 10 casos, envolvendo empresas e órgãos públicos. A partir dessa amostra iniciou-se o processo de abordagem das empresas/órgãos selecionadas através de

contato telefônico, utilização de *email*, com agendamento de visitas em dias e horários predefinidos. As empresas/órgãos que atenderam aos critérios definidos e que possibilitaram a realização da pesquisa foram cinco.

A primeira empresa, denominada neste texto por Empresa A, privada, pertence ao setor de segurança da informação; é brasileira e possui 18 anos de atuação no mercado. A Empresa A é fabricante nacional de soluções em segurança digital como *firewall*, antispam, centralizador de logs, VPN, IDS/IPS, filtro de conteúdo *web* e monitoramento remoto. Caracteriza-se por disponibilizar soluções no mercado na forma dual, ou seja, o mesmo produto utilizado para defesa cibernética é também comercializado nos mercados público e privado.

A segunda empresa selecionada para estudo, denominada Empresa B, privada, atua no mercado de segurança de pessoas e bens móveis desde 2008, é brasileira e fornece soluções tecnológicas para rastreamento de veículos via satélite (como rastreadores/bloqueadores de veículos, motos, frotas, cargas, pessoas e biometria veicular), através do uso de tecnologias como *Global Positioning System* (GPS), *General Packet Radio Service* (GPRS) e *Short Message Service* (SMS).

O primeiro órgão público selecionado para estudo, denominado Órgão Regulador A, compete organizar a exploração dos serviços de telecomunicações, em especial quanto aos aspectos de regulamentação e de seu acompanhamento, outorga de concessão e permissão, expedição de autorização, uso dos recursos de órbita e de radiofrequências, fiscalização e aplicação de sanções. O Órgão Regulador A possui uma Gerência de Certificação e Numeração responsável, além de outros serviços, pela certificação e homologação de produtos de comunicação e sistemas de telecomunicações, pela proposição de habilitação de laboratórios e de designação de organismos certificadores, além do controle da conformidade dos produtos de comunicação e sistemas de telecomunicações.

O segundo órgão público selecionado para estudo, denominado Órgão Regulador B, é uma autarquia federal, responsável por manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na qualidade de Autoridade Certificadora Raiz (AC-Raiz). Além de outras atribuições, é responsável pela condução dos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. (DOC-ICP-10). O Órgão Regulador B possui critérios específicos para Homologação e Certificação de equipamentos (*Hardware*) e sistemas (*Software*), em conformidade com as políticas estabelecidas pela Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil.

O terceiro órgão público selecionado para estudo, denominado Órgão Regulador C, pertence a Administração Federal Direta, tendo como missão o planejamento e coordenação das políticas de gestão da Administração Pública Federal - APF. Sendo o Departamento de Infraestrutura e Serviços de Tecnologia da Informação competente, dentre outras atribuições, pela normatização e promoção das coordenações quanto à infraestrutura de TI, definição dos processos e procedimentos de contratações de soluções de TI. O Órgão Regulador C encontra-se em processo de desenvolvimento do Programa Nacional de Homologação e Certificação de Ativos de TIC's para a APF.

O critério básico utilizado na coleta dos dados foi selecionar os profissionais relacionados à área de segurança da informação com experiência no processo de homologação/certificação do produto cibernético, seja o próprio gerente de projetos ou pessoas diretamente relacionadas ao processo de homologação e certificação de produtos.

No caso da Empresa A foram entrevistados dois profissionais envolvidos com o desenvolvimento do produto cibernético: um gerente de projetos e outro profissional da área de homologação de produtos. O acesso à documentação da Empresa A foi através do envio dos seguintes documentos: Modelo de Referência para Avaliação CERTICS (CTI ARCHER, 2013), RFC-2547 (SEMERIA, 2001), Manual do Produto IPS (AKER, 2016), Norma ISO/IEC 15504-2 (ABNT, 2008). No caso da Empresa B, o entrevistado foi o Diretor Comercial da empresa, com vasta experiência no produto cibernético em estudo. Apesar da Empresa B não ser desenvolvedora do produto é fornecedora do serviço de Rastreamento veicular através do Sistema de Monitoramento em Tempo Real.

No Órgão Regulador A, a entrevista foi realizada com um servidor diretamente relacionado à área de homologação e certificação de produtos. O acesso à documentação do Órgão Regulador A foi através de documentos obtidos através do próprio sítio web do órgão: Requisitos de Produtos Categoria II, Declaração de Conformidade, Instrução para Homologar Drones, Orientações para Certificar Produtos. No caso do Órgão Regulador B, a entrevista foi realizada com o Assessor de Direção, profissional bastante experiente na área de certificação e homologação de produtos, conhecedor e palestrante de vários temas na área de segurança. O acesso à documentação do Órgão Regulador B foi através de documentos obtidos através do próprio sítio web do órgão: (DOC-ICP-10), (DOC ICP-10.01), (DOC ICP-10.02), (DOC-ICP-10.05), (Manual de Condutas Técnicas 7, V. I) e (Manual de Condutas Técnicas 7, V. II).

Por último, no Órgão Regulador C, o entrevistado foi o Coordenador da Área de Especificação dos Requisitos de Avaliação de Conformidade (RACs) dos serviços de TICs

para a APF. O acesso à documentação do Órgão Regulador C foi através do envio dos seguintes documentos: Modelo de Governança e Gestão para a Auditoria de Segurança da Informação em Programas e Equipamentos, Requisitos de Avaliação de Conformidade do Correio Eletrônico, Requisitos de Avaliação de Conformidade de VoIP e Conjunto de características, Critérios, Condições Mínimas para Auditoria de Segurança da Informação.

O roteiro da entrevista seguiu quatro fases. Na primeira fase, o entrevistador apresenta o objetivo da pesquisa e o método de coleta de dados, com o objetivo de localizar o entrevistado diante do tema. Na segunda fase são coletados os dados do entrevistado, assim como um resumo de sua função dentro da empresa. Na terceira fase são coletadas informações sobre o produto cibernético em estudo. Na quarta fase inicia-se a obtenção das evidências com a aplicação de três formulários: Formulário de Análise do Processo de Homologação do Produto (APÊNDICE A), Formulário de Análise do Processo de Certificação do Produto (APÊNDICE B) e Formulário de Análise baseado na Norma ISO/IEC_15408: *Common Criteria for Information Technology Security Evaluation* (APÊNDICE C). No caso dos órgãos públicos, devido aos mesmos não serem fornecedores de produtos cibernéticos, a coleta de dados procurou identificar os procedimentos de homologação e certificação imputados pelos mesmos às empresas que fornecem os produtos que tais órgãos regulamentam.

As questões propostas nos formulários tiveram como objetivo a realização do diagnóstico da sistemática de homologação e certificação utilizada pelas empresas/órgãos para produtos/serviços cibernéticos. Além disso, possibilita identificar se os mesmos incluem em seus processos alguns dos requisitos para segurança do produto previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). As entrevistas tiveram a duração média de 1h e 50 min.

O Formulário de Análise do Processo de Homologação do Produto é composto por vinte e quatro perguntas. As perguntas são baseadas na fase de homologação do produto do MRM proposto por Barbalho (2006), incluindo questionamentos sobre protótipos, configurações e integração de *software* e *hardware*, especificação dos componentes mecânicos/eletrônicos, interfaces com a parte elétrica/eletrônica, documentação, identificação de falhas potenciais do produto, recursos de produção, dentre outros. Além disso, foram incluídas perguntas (15-20) referentes ao processo de verificação e validação de *software*.

Já o Formulário de Análise do Processo de Certificação do Produto é composto por seis perguntas baseadas na fase de validação do produto do MRM proposto por Barbalho (2006),

incluindo questionamentos do planejamento de certificação do produto, documentação exigida por órgãos certificadores, testes, procedimentos de submissão do produto à certificação, dentre outros. A validação do produto com o cliente presente na referida fase do modelo proposto por Barbalho (2006) não foi incluída no formulário, apenas os itens referentes à certificação do produto.

O Formulário de Análise baseado na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) é composto por oito perguntas relativas aos requisitos de segurança de produtos/serviços de TI descritos na Parte 3 (*Security assurance components*) da referida norma. As perguntas são baseadas nas seguintes Classes: Perfil de Proteção, Desenvolvimento, Documentação, Suporte ao Ciclo de Vida, Avaliação do Objetivo de Segurança, Testes e Análise de Vulnerabilidades. Além disso, o referido formulário inclui questionamentos sobre os Níveis de garantia para avaliação do produto (EAL1 a EAL7).

A partir dos dados coletados, iniciou-se a fase de Análise dos Dados. Os resultados dessa análise são descritos no item 4.6.

4.1 EMPRESA PRIVADA A

O produto da Empresa A é uma solução integrada de segurança da informação em *Software* do tipo IDS/IPS e filtro de aplicações, ou seja, apresenta em um só produto solução de detecção e prevenção de intrusões, além da filtragem de aplicações, cujo objetivo é proteger a integridade da rede de ameaças cibernéticas.

Além disso, o produto possibilita que o usuário detecte, identifique e execute ações preventivas em relação às ameaças cibernéticas, antes que essas possam causar danos potenciais, como, por exemplo, a exploração de falhas de segurança, violação de dados confidenciais, etc. O produto poderá ser adquirido de duas formas: *appliance* (*Hardware* com *Software* integrado) ou *Virtual Machine* (VM).

O *Software* apresenta uma interface chamada *Dashboard*, para facilitar o gerenciamento e visualização dos incidentes na rede. Permite ao administrador configurar componentes da interface gráfica conforme necessidades da empresa/ambiente, como, por exemplo, o total de eventos por protocolo, por prioridade de regra, Top 10 eventos por regra, Top 10 eventos por IP de origem, espaço utilizado em disco e uso de CPU.

A interface gráfica possui a aba “Eventos”, que permite ao usuário selecionar os parâmetros de pesquisa: Data inicial, Data final, Fluxo, Regra, Protocolo, IP de origem, IP de destino, Severidade e Página. Existe ainda uma terceira aba “NTOPNG”, que permite o

monitoramento e gerenciamento do tráfego da rede que, dentre outros recursos, oferece geração de relatórios para os seguintes protocolos: TCP, UDP, ICMP, (R) ARP, IPX, DLC, *Decnet*, *Apple Talk*, *Netbios* e TCP/UDP.

O protótipo é realizado através da utilização de *appliance* de rede para verificação da performance do *Software* e utiliza documentação de instalação que é desenvolvida junto com a homologação do produto, para os procedimentos necessários ao carregamento e testes do *Software*. Para o funcionamento do *Software* IPS são necessárias adaptações no *hardware* como tipo de memória, processador e 3 interfaces de rede: gerência, tráfego de entrada e tráfego de saída. Além disso, são necessários requisitos mínimos para o funcionamento do *Software* em relação ao *Throughput*: aproximadamente de 40 Mb/s HD de 160 GB; RAM de 4 GB; Processador de 2 núcleos de 1.6 Ghz (Intel D-510 CPU 1.6 Ghz). Para *Throughput* aproximadamente de 700 Mb/s, HD de 160 GB; RAM de 8 GB; Processador de 4 núcleos de 3 Ghz (Intel Core i3-2120 *Processor*). Já para a opção em *Virtual Machine* (VM) é necessário HD com capacidade de 20 GB e memória RAM de 8 GB.

Alguns procedimentos são realizados pela Empresa A para integração do *Software* ao *Hardware*, como o *Checklist* de homologação, em caso do resultado do *Checklist* ser aprovado o produto segue para a produção. Em caso de reprovação, o produto volta para o desenvolvimento. É o que acontece, por exemplo, com o *Display* LCD. Alguns componentes do produto são adquiridos com fornecedores através de uma lista de especificação de componentes. Existem interfaces com a parte elétrica/eletrônica, como, por exemplo, a placa de rede integrada à placa mãe. A Empresa A não define nenhum tipo de procedimento para a parte mecânica do produto. Já para a parte eletrônica existem documentos para aquisição, como descrições do tipo de memória e velocidade do processador. Além disso, são realizados testes de homologação para a montagem dos componentes da parte eletrônica, além de viabilizar a identificação de possíveis falhas potenciais no produto.

Para o desenvolvimento do produto, a Empresa A necessita de recursos como o desenvolvedor e homologador de produto, ferramentas de homologação, *Framework* de desenvolvimento e fornecedores de peças. A manutenção do produto é realizada pela própria empresa, em caso de *upgrade* de *Hardware/Software*. Existe um documento de *Checklist* realizado sobre os lotes dos fornecedores, o qual resulta em uma aprovação ou reprovação de peças. Para instalação e configuração de *Software* é necessário atendimento aos pré-requisitos do computador e verificação da versão do *software*. Em caso de *appliance*, poderá ser instalado de três formas distintas, visando atender empresas que utilizam redes pequenas,

médias e de grande porte. A Empresa A avalia a criticidade dos seus produtos e no caso do IPS a criticidade do *Software* é considerada de nível alto devido às consequências de um possível ataque à rede e comprometimento das informações.

Em se tratando das atividades para validação e verificação do *Software*, a Empresa A realiza um *Checklist* de verificação e valiação do *software*, passando por uma Comissão de Avaliação de Mudanças e por uma Comissão de Avaliação de Revisão (para adaptação ao mercado e às mudanças tecnológicas). A Empresa A oferece suporte técnico e treinamentos *online*, com certificação em seus produtos para o cliente final. Realiza ainda uma série de atividades para o desenvolvimento do *Software*. No caso de uma nova *release* de *software* oferece suporte técnico e manual, em caso de *bug* no produto, é feita uma avaliação com a equipe de desenvolvimento. A Empresa A adota as melhores práticas do guia PMBOK em suas atividades, como, por exemplo, na documentação da EAP, dicionário da EAP, definição do escopo e TAP. Além de possuir documentações como o Plano de Projeto de *Software*, manual de instalação do *Software*, casos de testes, oferece suporte do produto até o cliente e fórum de discussões.

Em relação aos testes do produto, a Empresa A possui ferramentas para testes para análise estática e conta ainda com uma ferramenta para análise dinâmica, a Avalanche. Os resultados dos defeitos detectados são documentados no próprio sistema e os resultados dos testes na ferramenta (*Bugzilla*). Em caso de análise dos impactos de mudanças no *Software*, a empresa adota os seguintes procedimentos: Revisão do *Checklist* de verificação e validação do *software*; Apoio pela Comissão de avaliação de mudanças; Avaliação de falsos positivos/falsos negativos; Análise de criticidade; Análise de migração de *Software*/*Hardware*; Análise de riscos e Atividades de integração de *Software/Software*: sistema operacional (SO) e outros sistemas, *Software/Hardware*. As alterações no banco de dados são analisadas quanto às falhas no *Software*, assim como os testes de regressão para análise de falhas no produto.

O controle da qualidade do produto na Empresa A é realizado através de um comparativo entre o que foi especificado e o que foi entregue ao cliente. A qualidade da homologação é realizada conforme o caderno de testes, incluindos os seguintes testes: independentes, regressão, funcionais, não-funcionais, aceitação, carga, performance, *stress* e confirmação, levando em consideração a quantidade de defeitos encontrados no *Software*. A fase de homologação do produto na Empresa A é concluída, no caso do protótipo, após a validação de todas as funcionalidades do produto, da seguinte forma: se o resultado das

funcionalidades do produto for aprovado o produto segue para a produção, caso contrário o produto volta para o desenvolvimento.

Neste caso, a versão final do produto será dada por concluída após a validação de todas as suas funcionalidades. Se o resultado das funcionalidades do produto for aprovado, serão escolhidos alguns clientes para receberem a versão "BETA" do produto para realização de testes e acompanhamento pela empresa. Se o resultado das funcionalidades do produto for reprovado, ele volta para o desenvolvimento. A homologação do produto é atestada através dos seguintes documentos: Casos de testes e relatório final de testes.

O processo de certificação na Empresa A é baseado nos procedimentos definidos no documento Metodologia de Avaliação da CERTICS para *Software* (CTI ARCHER, 2013), a estrutura do modelo segue os requisitos previstos na Norma ISO/IEC 15504-2 (ABNT, 2008). A Empresa A se planeja através de uma base de dados de avaliação, um *Checklist* de validação e pelo contrato de avaliação. Para a preparação documental do produto exigida por órgãos certificadores a Empresa A organiza toda a documentação gerada do produto. Para comprovar que o produto desenvolvido atende aos requisitos normativos aplicáveis, a Empresa A verifica a aderência entre *Hardware/Software* em relação ao que foi especificado.

A Empresa A possui um laboratório de testes na própria sede onde o produto é testado. Existe um ambiente para geração de tráfego (Servidores de injeção de tráfego) e para simulação do ambiente ao qual o produto irá operar, assim como um CPD de homologação com uma rede real controlada. A certificação do produto na Empresa A segue a Metodologia de Avaliação da CERTICS para *software*. Além disso, a Empresa A adota as melhores práticas do guia PMBOK para descrever os requisitos de *Software*, utiliza documentação para definição do produto e para análise de tráfego VPN, RFC-2547 (SEMERIA, 2001), documentação de segurança do produto e análise da segurança do código.

Para o desenvolvimento do produto, a Empresa A apresenta a documentação prevista na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), como, por exemplo: a descrição da arquitetura de segurança, especificação funcional e não funcional, representação da implementação (diagramas), funcionalidades de segurança interna do produto e projeto do produto. A Empresa A não adota o Modelo Formal da Política de Segurança previsto na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

Em relação à documentação do produto para o usuário final, a Empresa A fornece o Manual do Usuário, *Datasheet* com as características técnicas do produto e o Documento "*How To*" (como fazer). Durante o desenvolvimento e manutenção do produto são preparados

documentos como o TAP, controle de versões, definição do escopo, procedimentos de entrega, procedimentos para desenvolvimento seguro e controle de falhas no *Software*, modelo de desenvolvimento, além de utilizar ferramentas de apoio ao desenvolvimento do *Software* como os *frameworks* GIT e JIRA.

Para análise da segurança do produto, a Empresa A tem o apoio do Departamento de Serviços Avançados, além de utilizar ferramentas para análise do código e soluções para análise de vulnerabilidades. Os testes são realizados na própria empresa e o produto passa por diversos tipos de testes, dentre eles, testes independentes com empresas externas, regressão, funcionais e não funcionais, de aceitação do usuário, carga, performance, *stress* e confirmação.

As análises de vulnerabilidades do produto da Empresa A são realizadas no laboratório da empresa com uma ferramenta automatizada, além de utilização de outras ferramentas pelo Departamento de Serviços Avançados. O produto apresenta alto nível de criticidade devido à necessidade de poder ser instalado em um ambiente crítico, com acesso à *internet*, ponto de ocorrência de vulnerabilidades. Não foi observada a adoção de níveis de garantia de avaliação do produto.

4.2 EMPRESA PRIVADA B

O produto cibernético da Empresa B é uma tecnologia embarcada em dispositivos veiculares cuja função é o rastreamento de veículos, incluindo o Sistema de Monitoramento em Tempo Real, o qual permite a localização do veículo via GPS/GPRS e é regulamentado pela Portaria do Departamento Nacional de Trânsito - Denatran nº 253/2009. São elementos mandatórios desse tipo de produto: Módulo de Recepção Satélite, Módulo de Comunicação Bi-direcional (deverá possuir o certificado de homologação da Agência Nacional de Telecomunicações - Anatel), Módulo de Bateria Auxiliar e Módulo de Gerenciamento e Bloqueio.

O SIMCard é conectado à placa eletrônica do *hardware* que é instalado dentro do veículo. Através do SIMCard as informações do veículo são enviadas para as antenas as quais transmitem as informações para os servidores da Empresa B, os quais compilam essas informações para o computador alimentando o Sistema de Monitoramento em tempo real.

Além de restrear e fornecer a localização do veículo, o produto poderá agregar informações de Telemetria, como, por exemplo: velocidade (média e máxima), hodômetro, RPM, consumo médio, aviso de bateria, dados de sensores (Ignição, Porta do motorista, Porta

do carona, Desengate), dados de atuadores (Bloqueio, Sirene, Setas, Trava de baú), etc. Dentre os itens de segurança estão o botão de pânico para comunicação de eventos anormais (sequestro, assalto, acidente, etc.), monitoramento da situação do motor, do baú, das portas, além de traçar o perfil do condutor do veículo. Possibilita ainda configurar o tempo de envio dos dados de localização e telemetria ao Sistema de Monitoramento conforme a necessidade do cliente.

A Empresa B, não desenvolve o produto, recebe diretamente do fabricante com os testes de fábrica já realizados. Após receber o produto a Empresa B realiza testes nos componentes na própria empresa, mas não há registro de documentação. Existem algumas configurações iniciais realizadas no *Hardware* para o funcionamento do *Software*, como: IP, Porta, parâmetros do APN (*Access Point Names*) protocolo de comunicação das redes GSM e configurações no endereço do SIMCard. Pode-se configurar quais serviços embarcados estarão ativos para um determinado veículo, como, por exemplo, o bloqueio de sirene, função *Jamming*, a qual impede o estabelecimento de comunicação em uma determinada faixa de frequências, dentre outros.

Algumas características de *hardware* são essenciais para o funcionamento do *Software* como o relé para o bloqueio e os sensores para o controle da temperatura. O Sistema de Monitoramento funciona via Internet e Celular para (Android, IOS). Os componentes mecânicos são definidos pelo fabricante e as especificações para aquisição vão depender da demanda do mercado podendo apresentar diversas linhas de equipamentos.

A Empresa B não possui procedimentos para aquisição ou fabricação de componentes mecânicos/eletrônicos, pois há apenas os procedimentos de montagem do produto no veículo através do Manual de Instalação, realizado pelo próprio técnico da empresa. Os testes são realizados antes da montagem (instalação) do produto no veículo e incluem um *checklist* completo, verificando a parte elétrica em busca de possíveis anomalias. Uma vez instalado no veículo o usuário não tem mais contato com o equipamento, apenas através do monitoramento via *Software*, motivo pelo qual a empresa não oferece manual ao usuário final. Em caso de falhas de comunicação no sistema GPS/GPRS pelo veículo monitorado, a Empresa B possui um procedimento específico para bloqueio do veículo, o qual não foi detalhado durante a entrevista. Todos os componentes do produto da Empresa B são fornecidos pelo fabricante.

A criticidade do *software* da Empresa B, conforme relato do entrevistado, pode ser considerada alta, devido ao fato de envolver além da segurança de um bem material a própria vida do condutor em caso de sequestro. Porém, não há informações do fabricante sobre a

adoção de níveis de criticidade de s*oftware.* O sistema possui aviso sonoro audível e diversos tipos de mapas de visualização satelital para facilitar a localização do veículo. A Empresa B não adota atividades relacionadas ao gerenciamento da validação e verificação do *software*, nem para o desenvolvimento do mesmo. Em relação aos testes, a Empresa B realiza testes da parte elétrica do veículo, já com o produto instalado ao mesmo, porém não possui nenhuma ferramenta para automação dos testes. Os testes elétricos são realizados por técnicos devidamente habilitados.

Ao ser detectado algum tipo de defeito no produto é gerada uma nota de devolução ao fabricante solicitando a reposição da peça e documentado através do *check-list*. Em casos de verificação de melhorias no *software* ou adaptações é preenchida uma Ficha de Mudanças e enviada ao fornecedor do produto. O controle da qualidade é medido através do número de veículos localizados pelo Sistema de Monitoramento e a eficácia das funções de segurança do produto como bloqueio, travamento, acionamento do alarme, dentre outras. A homologação do produto na Empresa B é realizada após o resultado satisfatório dos testes através de um *Checklist* de testes.

O produto da Empresa B é homologado e certificado pelos respectivos órgãos Anatel e Centro de Experimentação e Segurança Viária - Cesvi Brasil. As atividades iniciais para o planejamento da certificação do produto não são realizadas pela Empresa B, sendo responsabilidade do fabricante.

Devido ao fato da Empresa B não ser desenvolvedora do produto, a mesma não apresenta uma documentação para desenvolvimento seguro como previsto no Perfil de Proteção citado pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). A Empresa B não oferece documentação do produto para o usuário final, pois uma vez instalado no veículo, o usuário tem contato restrito com o produto, apenas por meio do Sistema de Monitoramento. O usuário terá apoio através da Central de Monitoramento para comunicação de ocorrências sobre o sinistro do veículo.

A Empresa B oferece o Manual de Instalação para técnicos responsáveis pela instalação do produto no veículo. Antes da instalação é realizado o preenchimento de um *checklist* completo, que passa por verificações elétricas apontando possíveis anomalias. Em relação aos controles para manutenção do produto previstos no Ciclo de Vida do Produto, a Empresa B gerencia configurações do produto para adequação aos serviços adquiridos pelo usuário e identificação dos itens de configuração. Não há ferramentas para o desenvolvimento nem análise do produto. Para receber o produto o cliente leva o veículo até a empresa onde são

realizados os procedimentos de instalação e testes no mesmo, por este motivo a Empresa B não possui procedimentos de "*Delivery*" do produto ao usuário.

A segurança do produto é verificada através dos testes realizados em laboratórios do Cesvi Brasil, para que o produto possa receber a certificação. O *Software* é analisado em relação aos itens de monitoramento, porém não há informações de realização de testes para análise de vulnerabilidades no *software* de Monitoramento. Não há informações sobre níveis de garantia de avaliação do produto.

A seguir serão exibidos os dados da coleta dos Formulários de Análise do Processo de Homologação e Certificação do produto nas Empresas privadas A e B. Por último serão exibidos os dados coletados do Formulário de Análise baseado na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) nas Empresas A e B.

Quadro 1 - Itens do Formulário de Análise do Processo de Homologação do Produto em Empresas Privadas

Itens do Formulário de Análise do Processo de Homologação do Produto em Empresas Privadas		
ITENS	**Empresa A**	**Empresa B**
1. Protótipo	*Appliance* de rede	Fabricante
2. Carregamento e Teste do *Software*	Adota em documentação	Não Adota
3. Configurações no *Hardware*	Memória, processador e interface	IP, Porta, APN (*Access Point Name*)
4. Características de *Hardware*	Memória, processador e 3 interfaces de rede	Bloqueio: relé Temperatura: sensores
5. Integração do *Software* ao *Hardware*	*Checklist* de homologação	Fabricante
6. Especificação dos Componentes Mecânicos e Interfaces Elétrica/Eletrônica	Lista de especificação. Placa de rede integrada a placa mãe.	Fabricante
7. Procedimentos de montagem e manufatura dos Componentes Mecânicos	Não adota	*Checklist* de montagem
8. Procedimentos de montagem e manufatura dos Componentes Eletrônicos	Adota documentos para aquisição, descrições do tipo de memória e velocidade do processador.	Não Adota
9. Procedimentos de revisão dos Componentes Mecânicos (listas de peças e componentes de cada parte, subsistema, e submontagem do produto)	Não adota	Procedimentos de testes (Parte elétrica)
10. Procedimentos de revisão dos Componentes Eletrônicos (listas de componentes eletrônicos, de gerbers para fabricação das peças, procedimentos de montagem eletrônica e revisão da documentação de teste da eletrônica)	Testes de homologação	Não Adota
11. Falhas do Produto	Testes de homologação	Não Adota (Notifica o fabricante)
12. Recursos de Produção do Produto	RH; Ferramentas; *Framework* de desenvolvimento e Fornecedores de peças	Fabricante
13. Fornecedores	*Upgrade* de *Hardware/Software* e *Checklist* dos lotes dos fornecedores	Fabricante
14. Instalação e configuração do *Software*	Pré-requisitos do computador versão do *software*	*Internet*
15. Criticidade do *Software*_IEEE 1012	Adota. Produto IPS (ALTA)	Fabricante

Itens do Formulário de Análise do Processo de Homologação do Produto em Empresas Privadas		
ITENS	**Empresa A**	**Empresa B**
16. Validação e verificação do *Software*_IEEE 1012	1. *Checklist* de verificação e valiação*;* 2. Comissão de avaliação de mudanças; 3. Comissão de avaliação de revisão; 4. Suporte técnico e 5. Treinamentos *online* e certificação	Não Adota
17. Desenvolvimento do *Software*_IEEE 1012	1.Nova *release* de *software*: suporte técnico e manual; 2. *Bug* do produto: avaliado; 3.Melhores práticas do PMBOK; 4. Plano de projeto de *Software*; 5.Manual de instalação do *Software*; 6. Fórum de discussões; 7. Casos de testes 8. Suporte do produto ao cliente.	Não Adota
18. Testes_IEEE 1012	Ferramentas para análise estática e dinâmica; Ferramenta para automação: (Avalanche)	Realiza testes da parte elétrica do veículo com o produto instalado.
19. Documentação dos Testes_IEEE 1012	Ferramenta: *Bugzilla*	Através de um *Checklist* da parte elétrica do veículo.
20. Impactos de mudanças no *Software*_IEEE 1012	1. Revisão do *Checklist* de verificação e valiação do *software*; 2. Comissão de avaliação de mudanças; 3. Avaliação de falsos positivos/ negativos; 4. Análise de criticidade; 5. Análise de migração de *Software*/*Hardware*; 6. Análise de riscos; 7. Atividades de integração de *Software/Software*: sistema operacional (SO) e outros sistemas, *Software/Hardware*.	Ficha de Mudanças (enviada ao Fornecedor)

Itens do Formulário de Análise do Processo de Homologação do Produto em Empresas Privadas		
ITENS	**Empresa A**	**Empresa B**
21. Alterações de Projeto	Alterações no BD: falhas no *Software*; Testes de regressão: falhas no produto	Não Adota
22. Controle da Qualidade	Comparativo: (especificado e entregue); Qualidade: caderno de testes (quantidade de defeitos encontrados no *Software*)	Número de veículos localizados pelo Sistema de Monitoramento e eficácia das funções do produto
23. Conclusão da Homologação	Protótipo: após a validação de todas as funcionalidades do produto; Versão final do produto: Aprovado: clientes recebem vrs. "BETA"; Reprovado: o produto volta para o desenvolvimento.	Após o resultado "satisfatório" dos testes
24. Documentos de Homologação	*Checklist* de homologação; Plano de testes; Casos de testes; e Relatório final de testes.	*Checklist* dos testes

Fonte: Elaborado pelo autor

Quadro 2 - Itens do Formulário de Análise do Processo de Certificação do Produto em Empresas Privadas

Itens do Formulário de Análise do Processo de Certificação do Produto em Empresas Privadas		
ITENS	**Empresa A**	**Empresa B**
1. Planejamento da Certificação	Metodologia de Avaliação CERTICS para *Software* ABNT NBR ISO/IEC 15504-2 (2008): Tecnologia da Informação	Fabricante Certificações: Cesvi Brasil e Anatel.
2. Documentos para Planejamento da Certificação	1.Base de dados de avaliação; 2.*Checklist* de valiação; 3.Contrato de avaliação.	Não Adota
3. Documentação do Produto para Órgãos Certificadores	Análise dos resultados esperados. Não são exigidas documentação	Não Adota
4. Conformidade do Produto aos Requisitos Normativos	Verificação da aderência do *Hardware/Software* em relação ao que foi especificado.	Não Adota
5. Testes (Como e Local)	Existe um ambiente de geração de tráfego (Servidores de injeção de tráfego) para simular o ambiente ao qual o produto irá operar. CPD de homologação com uma rede real controlada. Local: laboratório de testes na própria empresa.	- Testes em fábrica; - Testes dos componentes na empresa; e - Testes nos órgãos certificadores.
6. Certificação do Produto	Certificação CERTICS: 1. Método de Avaliação: Fase1-Exploração, Fase2-Contratação Fase3-Preparação, Fase4-Visita Fase5-Validação, Fase6-Conclusão 2. Processo de Certificação: Submete um pleito à SEPIN/MCTI para Emissão do Certificado.	Fabricante

Fonte: Elaborado pelo autor

Quadro 3 - Itens do Formulário de Análise Baseado na Norma ISO/IEC_15408 em Empresas Privadas

Itens do Formulário de Análise baseada na Norma ISO/IEC_15408 em Empresas Privadas		
ITENS	**Empresa A**	**Empresa B**
1. Protection Profile (PP): (1) PP Introduction; (2) Conformance Claims; (3) Security Problem Definition; (4) Security Objectives; (5) Extended Components Definition e (6) Security Requirements.	Adota DOC's para os itens (1), (3) e (4) (2) RFC-2547 (5) RFC-2547	Não adota a documentação, apenas verifica se os parâmetros de segurança são atendidos.
2. Documentação para o Desenvolvimento do Produto: (1) Security Architecture; (2) Functional specification; (3) Implementation representation; (4) TSF internals; (5) Security policy modelling; e (6) TOE design	Adota DOC's itens (1), (2), (3), (4) e (6) (5) Não Adota	Fabricante
3. Documentação para o Usuário Final (1) Operational user guidance e (2) Preparative procedures	Adota	(1) Não Adota (2) DOC
4. Controles de Desenvolvimento e Manutenção do Produto (1) CM capabilities; (2) CM scope; (3) Delivery; (4) Development security; (5) Flaw remediation; (6) Life-cycle definition e (7) Tools and techniques.	Adota DOC's para os itens (2),(3),(4) e (6) (5) Ferramenta *Bugzilla* (7) GIT/JIRA	Adota (1) e (5) mas não documenta.
5. Segurança (1) ST Introduction; (2) Conformance claims; (3) Security problem definition; (4) Security objectives; (5) Extended components definition; (6) Security requirements e (7) TOE summary specification.	Adota DOC's para os itens (1), (2), (3), (4), (6) (7). (5) Não observado	Não há informações
6. Testes (1) Testes de cobertura; (2) Testes de profundidade (Depth Tests); (3) Testes independentes (Independent Tests) e (4) Testes funcionais (Functional Tests).	Adota (1), (2), (3), (4). Inclui regressão, carga, performance, *stress* e confirmação.	Laboratórios do Cesvi Brasil itens de monitoramento (1) e (2).
7. Análise de Vulnerabilidades (1) Vulnerability Survey; (2) Vulnerability Analysis; (3) Focused Vulnerability Analysis; (4) Methodical Vulnerability Analysis; (5) Advanced Vulnerability Analysis.	Adota (4) Departamento de Serviços Avançados	Não há informações
8. Níveis de garantia de Avaliação do Produto EAL1, EAL2, EAL3, EAL4, EAL5, EAL6 e EAL7	Não há informações	Não há informações

Fonte: Elaborado pelo autor

4.3 ÓRGÃO REGULADOR A

O produto cibernético em estudo no Órgão Regulador A são os Veículos Aéreos Não Tripulados (VANT), também conhecidos como “Drones”, nome genérico, sem amparo técnico. Utilizado inicialmente pelo Exército, também estão presentes em atividades industriais, comerciais, para resgate em locais de difícil acesso, dentre outras. (PORTAL BRASIL, 2015). Dentre os vários componentes de um “Drone”, estão presentes: microcontrolador, processador (para leitura das informações dos sensores), memória, *software*, sensores para indicação do nível de inclinação do Drone (giroscópio e acelerômetro), motor, GPS (para controle de navegação em alguns modelos), dentre outros.

A Certificação e Homologação de produtos do Órgão Regulador A de fabricantes nacionais ou estrangeiros a serem comercializados no Brasil segue a Resolução nº 242/00 da Anatel, a qual divide os produtos do Órgão Regulador A em três categorias. Na Categoria I estão incluídos os equipamentos terminais destinados ao uso do público em geral, para acesso a serviços de telecomunicações de interesse coletivo. Já a Categoria II inclui produtos não incluídos na Categoria I, mas que utilizam do espectro radioelétrico para transmissão de sinais, incluindo neste caso as antenas e equipamentos de radiocomunicação de radiação restrita. Na Categoria III estão os produtos não incluídos nas categorias anteriores, cuja regulamentação seja necessária para garantir a interoperabilidade, confiabilidade das redes e compatibilidade eletromagnética. No caso dos “Drones”, o controle remoto que opera o mesmo está incluído na Categoria II, sendo tratado como Equipamento de Radiocomunicação de Radiação Restrita (Resolução nº 506/08 da Anatel). O Órgão Regulador A define os requisitos técnicos e procedimentos de ensaios aplicáveis à certificação de produtos para cada uma de suas categorias.

Os Equipamentos de Radiocomunicação de Radiação Restrita podem ser definidos como equipamento, aparelho ou dispositivo, o qual utiliza radiofrequência para aplicações diversas em que a correspondente emissão produza campo eletromagnético com intensidade dentro dos limites estabelecidos conforme a Resolução nº 506/08 da Anatel. Estes equipamentos devem possuir certificação emitida pelo Órgão Regulador A ou aceita pelo mesmo, a qual deverá constar a condição de radiação restrita conferida ao mesmo, bem como a indicação da máxima intensidade de campo em uma determinada distância e o tipo de elemento radiante permitido na utilização do equipamento.

As estações de radiocomunicação correspondentes a esse tipo de equipamento operam em caráter secundário, ou seja, não possuem direito à proteção contra possíveis interferências prejudiciais provenientes de qualquer outra estação de radiocomunicação. Além disso, não podem causar interferência em qualquer sistema operando em caráter primário. As faixas de frequências não permitidas para utilização de equipamentos de radiação restrita, assim como a intensidade de campo são definidas na Resolução nº 506/08 da Anatel.

Os procedimentos de ensaios para os Equipamentos de Radiocomunicação de Radiação Restrita são descritos no Ato nº 1135/13 da Anatel. Os aspectos de compatibilidade eletromagnética são descritos na Resolução nº 442/06 da Anatel e os de segurança elétrica na Resolução nº 529/09 da Anatel. Os princípios dos processos de certificação e homologação de produtos do Órgão Regulador A deverão dentre outros, asseguar que os fornecedores atendam aos requisitos mínimos de qualidade, segurança e de não agressão ao ambiente para seus produtos. Caso necessário o Órgão Regulador A poderá exigir a realização de testes de campo do produto ou equipamento, de forma a obter subsídios para sua decisão quanto à oportunidade ou viabilidade da certificação (Resolução nº 242/00 da Anatel).

O Órgão Regulador A poderá estabelecer, os requisitos ou normas técnicas a serem aplicadas ao processo de avaliação da conformidade, como, por exemplo, normas técnicas nacionais ou internacionais, regulamentos aplicáveis ao produto em outros países ou regiões, regulamentos editados pelo próprio Órgão Regulador A para produtos similares e especificações do fabricante. Em se tratando dos produtos utilizados pelas Forças Armadas, os quais empregam radiofrequências nas faixas destinadas a fins exclusivamente militares, estarão dispensados de certificação ou homologação pelo Órgão Regulador A (Resolução nº 242/00 da Anatel).

Os Drones podem ser homologados pelo Órgão Regulador A de duas formas distintas, a primeira é realizada quando o interessado deseja homologar com fins de comercialização do equipamento. Este tipo de homologação é chamado de “Homologação por Certificação de Conformidade”. Fabricantes que desejam comercializar Drones se encaixam nessa forma. Por outro lado, quando o interessado importa ou fabrica um equipamento emissor de radiofrequência voltado para uso próprio é chamada de “Homologação por Declaração de Conformidade”. Conforme o Órgão Regulador A, a Declaração de Conformidade deverá indicar os regulamentos ou as normas aplicáveis ao

produto e atestar que o mesmo está em conformidade com os regulamentos ou normas aplicáveis.

Quando a parte interessada for o próprio usuário do produto, deverá estar explícito na "Declaração de Conformidade" que a utilização do equipamento dar-se-á em conformidade com as características técnicas objeto da declaração. A Homologação e Certificação de "Drones" através da "Homologação por Declaração de Conformidade" poderá ser realizada através do cadastro no Sistema de Gestão de Certificação e Homologação (SGCH) do Órgão Regulador A. Neste sistema o interessado deverá informar os requerimentos para homologação de produtos de telecomunicações e os dados do "Drone".

Além disso, deverá escolher a opção "Transceptor de Radiação Restrita", e no campo serviços a opção "Radiocomunicação de Radiação Restrita", com a informação dos dados técnicos do produto. A "Declaração de conformidade do produto" deverá assegurar que o produto atende aos requisitos técnicos aplicáveis conforme lista disponível no *sitio* do Órgão Regulador A. A utilização do produto deverá atender às condições estabelecidas pelo Departamento de Controle do Espaço Aéreo - DECEA e pela Agência Nacional de Aviação Civil – ANAC.

Para comprovação da conformidade perante o Órgão Regulador A, o interessado deverá apresentar um dos seguintes documentos: Declaração de Conformidade, Declaração de Conformidade com relatório de ensaio, Certificado de Conformidade baseado em ensaio de tipo (Categoria III), Certificado de Conformidade baseado em ensaio de tipo e em avaliações periódicas do produto (Categoria II) ou Certificado de Conformidade com avaliação do sistema da qualidade (Categoria I), para obter o Certificado de Homologação do produto. O fluxo do processo para Certificação e Homologação de produtos no Órgão Regulador A, considerando a "Homologação por Certificação de Conformidade", pode ser descrita através dos seguintes itens:

a. O Fabricante nacional ou representante seleciona um Organismo de Certificação Designado (OCD) e fornece as informações técnicas sobre o produto.
b. O OCD analisa o produto e suas características e determina os padrões e ensaios aplicáveis.
c. O Fabricante nacional ou representante escolhe um laboratório e fornece uma amostra do produto, acompanhada de uma declaração do fabricante, indicando ter sido coletada na produção. Existem 2 tipos de laboratórios: (a)

Laboratórios de Ensaio Acreditados: São organismos acreditados pelo Inmetro, no âmbito específico das telecomunicações e (b) Laboratório de Ensaios Avaliados: São organismos não acreditados pelo Inmetro, porém são avaliados conforme critérios estabelecidos pelo Órgão Regulador A.

d. O laboratório executa os ensaios previstos na regulamentação e emite o Relatório do Ensaio.
e. O OCD analisa os resultados do ensaio, emite o Certificado de Conformidade e o cadastra no Sistema de Gestão de Certificação e Homologação (SGCH) do Órgão regulador A.
f. O Órgão Regulador A analisa toda a documentação e emite o Certificado de Homologação.

O órgão Regulador A descreve os Equipamentos de Radiocomunicação de Radiação Restrita através da Resolução nº 506/08; além disso recomenda ao fabricante a conformidade com os requisitos de compatibilidade eletromagnética de seus produtos através da Resolução nº 442/06 e segurança elétrica através da Resolução nº 529/09, as quais são semelhantes ao documento sugerido pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), perfil de proteção para uma classe de produtos. Além disso, orienta que os produtos oferecidos pelo comércio deverão apresentar um padrão mínimo de qualidade e adequação aos serviços a que se destinam, incluindo requisitos de segurança e não agressão ao ambiente.

4.4 ÓRGÃO REGULADOR B

O produto cibernético em estudo no Órgão Regulador B são os Módulos de Segurança Criptográficos (MSC, também conhecidos como HSM – *Hardware Security Modules*) e podem ser definidos como dispositivos de criptografia baseado em *hardware*, seguro e resistente à violação. Este produto provê funcionalidades criptográficas capazes de gerar, armazenar e proteger chaves criptográficas simétricas e assimétricas para aplicação em uma Infraestrutura de Chaves Públicas (ICP Brasil, DOC-ICP-10.05)

Neste tipo de *hardware,* a fronteira criptográfica define um perímetro no qual estão presentes componentes como processadores, memórias, assim como outros dispositivos de *hardware, software* e *firmware.* A fronteira criptográfica também é delimitada através de mecanismos de segurança física visando à proteção destes componentes contra sondagem,

observação e manipulação direta. Este produto provê segurança através da conformidade com alguns padrões de construção de *Hardware* e de requisitos de projeto, como a FIPS PUB 140-2 (NIST, 2001), ISO/IEC_15408 (COMMON CRITERIA, 2012) e Manuais de Condutas Técnicas (MCT-7, V. II) da ICP-Brasil.

A Figura 17 mostra um modelo do Módulo de Segurança Criptográfico (MSC) desenvolvido por um fabricante nacional, o qual possui certificado ICP-Brasil MCT 7 NSH3 e NSF2, compatível com a FIPS-140 nível 4. Dentre as várias aplicações para este tipo de produto estão as Infraestruturas Críticas e Defesa (Marinha, Exército e Aeronáutica).

Figura 17 - Módulo de Segurança Criptográfico AHX4 ASI-HSM

Fonte: KRYPTUS, 2016

Os critérios para homologação e certificação de equipamentos (*Hardware*) e sistemas (*Software*) do Órgão Regulador B estão em conformidade com as políticas estabelecidas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O processo de homologação do Órgão Regulador B tem por objetivo assegurar aos equipamentos os padrões e especificações técnicas estabelecidos pelas normas da ICP-Brasil, conforme previsto na norma DOC-ICP-10. A parte interessada na homologação de um sistema ou equipamento de certificação digital no âmbito da ICP-Brasil, deverá entregar o Laudo ou Certificação de Conformidade do sistema ou equipamento com a respectiva documentação: Termo de Propriedade Intelectual, Documentos Comprobatórios, Laudo ou Certificado de Conformidade e Termo de Sigilo.

O processo de homologação no Órgão Regulador B para MSC visa assegurar a interoperabilidade e operação segura do serviço criptográfico ICP oferecido por um MSC através da avaliação técnica de aderência aos requisitos técnicos definidos para este processo. São requisitos a serem observados no processo de homologação dos MSC: (1) Aderência aos requisitos de segurança, gerenciamento, restrição de substâncias nocivas e (2) Aderência à interfaces de interoperabilidade específicas, das quais pelo menos uma

deverá ser suportada: PKCS#11, CryptoAPI, JCE, OpenSSL, API proprietária (caso utilizada) informando o ambiente operacional no qual foi analisada a interoperabilidade (ICP BRASIL, 2007).

O Órgão Regulador B adota níveis de segurança de homologação e define graus de confiabilidade nos resultados obtidos a partir dos ensaios realizados pelo laboratório credenciado. O nível deverá constar no laudo de conformidade a ser emitido pelo Laboratório de Ensaios e Análises (LEA). A parte interessada pelo processo de homologação deverá fornecer o nível de segurança de homologação (NSH) desejado para o produto. Os níveis de segurança de homologação conforme a norma DOC ICP-10.02 são: NSH1, NSH2 e NSH3.

Aplica-se o nível NSH1 em situações onde há necessidade de operação correta do sistema ou equipamento, porém as ameaças à segurança ao ambiente de utilização dos mesmos estão controladas, sendo os problemas de interoperabilidade não relevantes neste caso. A avaliação neste nível é básica e a parte interessada deverá fornecer a documentação básica do produto. Incluem testes de funcionalidade, porém não é necessário a disponibilidade do código-fonte. Para o nível NSH2 está previsto um ambiente onde as ameaças à segurança e problemas de interoperabilidade são relevantes e necessita-se de confiança no sistema. Neste nível, a avaliação é moderada, incluindo depósito de amostras do objeto de homologação, resultados dos testes e depósito do código-fonte. No nível NSH3 a avaliação é considerada alta, devido as ameaças à segurança serem críticas, sendo indispensável a confiança na operação correta do sistema. Neste nível, além do fornecimento de informações de projeto pela parte interessada como resultados de testes e depósito dos códigos-fonte, é necessária a comprovação da utilização de práticas seguras para o desenvolvimento e produção.

Além dos níveis de homologação, o Órgão Regulador B estabelece dois níveis de segurança física: NSF1 e NSF2. O nível NSF1 requer que o Módulo de Segurança Criptográfico suporte no mínimo os mecanismos de segurança física que resistam à violação. Já o nível NSF2 além de contemplar os mecanismos de segurança física previstos no NSF1, requer que o MSC suporte ainda mecanismos de segurança física que detectam e respondam à violação.

O processo de homologação de produtos do tipo HSM realizado pelo Órgão Regulador B se inicia com a busca por uma OCP pela parte interessada (Fornecedor ou Fabricante). A OCP conduz o processo de certificação e envia o Certificado de Conformidade do produto fornecido por um dos laboratórios acreditados ao Órgão

Regulador B, atestando adequação aos Requisitos de Avaliação de Conformidade (RAC) para equipamentos de Certificação Digital Padrão ICP-Brasil normatizado pelo INMETRO.

Recebida a documentação enviada pela OCP, o Órgão Regulador B inicia a análise quanto à homologação do equipamento solicitado. Em caso do Certificado de Conformidade atender aos requisitos obrigatórios para um equipamento, a homologação constituirá Ato Declaratório do diretor de Infraestrutura de Chaves Públicas do órgão Regulador B que será publicado no Diário Oficial da União. Assim, o Fornecedor/ Fabricante solicitante receberá autorização para uso do Selo de Homologação e do correspondente número de identificação do equipamento. Porém, quando o Certificado de Conformidade apresentar alguma não-conformidade a qualquer um dos requisitos obrigatórios para o equipamento, a homologação será indeferida. São entidades do processo de homologação no âmbito da ICP-BRASIL: Órgão Regulador B, Laboratórios de Ensaios e Auditoria (LEA), Parte Interessada, Organismo de Certificação de Produto (OCP) e Laboratórios Acreditados (aptos a realizarem os ensaios no âmbito da ICP-Brasil).

A Portaria nº 8 de 2013 do Inmetro estabelece critérios para o Programa de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil, os quais são compulsórios, atendendo aos requisitos dos Manuais de Conduta Técnica 1, 2, 3 e 7, Volumes I e II, e DOC-ICP-01.01 e aos Requisitos Gerais de Certificação de Produtos (RGCP).

O órgão Regulador B adota três níveis de Segurança de Certificação, os quais possuem diferentes graus de confiabilidade nos resultados de ensaios realizados pelo laboratório acreditado. O Nível 1 (NSC1) requer confiança na correta operação do equipamento, contudo as ameaças à segurança no ambiente devem ser controladas e fatores como eventuais problemas de interoperabilidade não são relevantes. Para este Nível a avaliação é básica e os testes realizados incluem funcionalidades do produto conforme especificações do fornecedor e da avaliação da documentação fornecida. Por outro lado, o Nível 2 (NSC2) é adequado quando se requer confiança na correta operação do Equipamento e o ambiente apresenta ameaças relevantes à segurança, assim como problemas de interoperabilidade.

Já para o Nível 3 (NSC3), é apropriado quando se necessita de confiança na operação correta do Sistema ou Equipamento, cuja utilização está prevista em ambiente no qual as ameaças à segurança ou problemas de interoperabilidade são considerados críticos. Neste Nível a avaliação é realizada com cobertura alta, através do depósito de amostras do objeto

de certificação e baseada no fornecimento de informações mais detalhadas do projeto, resultados de testes já realizados, depósito de todo o código fonte e comprovação da utilização no produto de práticas para garantia da segurança.

No processo de homologação dos MSC devem ser verificados os requisitos técnicos de Especificação, Segurança, Interoperabilidade, Gerenciamento, Funcionais e Documentação. Alguns requisitos de segurança são derivados do padrão FIPS 140-2 (NIST, 2001), como por exemplo, documentação do módulo criptográfico e identificação de portas e interfaces os quais são semelhantes ao documento perfil de proteção para uma classe de produtos, previsto na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Além disso, o padrão americano inclui itens para níveis de segurança física para o produto (NSF1 e NSF2), interferência e compatbilidade eletromagnética, Mitigação de outros ataques similiares respectivamente às seguintes classes da Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), segurança, testes e análise de vulnerabilidades.

Além disso, estão previstos itens de gerenciamento, operacionalidade, restrição à substâncias nocivas (RoHS) e obrigatoriedade como alguns algoritmos criptográficos. Os testes dos MSC além dos derivados do padrão FIPS 140-2 (NIST, 2001) incluem energização e condicionais (Testes de consistência de pares, se o módulo criptográfico gera chaves públicas e privadas); Testes de carregamento de *Software*/*Firmware*; Testes de entrada manual de chaves; Teste do gerador de números aleatórios do tipo “contínuo” (*continuous test*) para o gerador de números aleatórios por *hardware*, dentre outros). Observa-se que os referidos testes apresentam semelhança aos descritos na classe Testes, prevista na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Além disso, o Órgão Regulador B adota três níveis de certificação do produto (NSC1, NSC2 e NSC3) semelhantes aos níveis de garantia de avaliação do produto (EAL1 a EAL7) previstos na referida norma.

4.5 ÓRGÃO REGULADOR C

No âmbito da Administração Pública Federal - APF, informação e tecnologia são considerados ativos estratégicos e indispensáveis à prestação do serviço público. Dessa forma, a segurança da informação e comunicações é item prioritário dos órgãos e entidades da APF que são consideradas complexas, empregando grande volume de informações para prestação do serviço público ao cidadão. De acordo com o Modelo de Governança e Gestão para a Auditoria de Segurança da Informação em Programas (2015) e equipamentos

problemas de segurança que colocam em risco a disponibilidade, integridade, confidencialidade e autenticidade necessitam de ações permanentes nas organizações governamentais.

O Modelo de Governança e Gestão desenvolvido pelo Órgão Regulador C representa uma proposta inicial para especificações técnicas, premissas e diretrizes referentes às características que possibilitem auditoria de segurança da informação em programas e equipamentos, cujo propósito é garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações de ativos adquiridos pelo Governo Federal de acordo com o Decreto nº 8.135/13. O referido modelo visa contemplar características genéricas essenciais para todos os seviços citados na normativa vigente e em outros que possam surgir. Vale ressaltar que o referido documento não tem o propósito de um processo de certificação, devido a cada classe de dispositivo (programa/equipamento) demandar avaliação de outras entidades envolvidas como por exemplo o Serviço Federal de Processamento de Dados- SERPRO, Empresa de Tecnologia e Informações da Previdência Social - DATAPREV, Telecomunicações Brasileiras S.A. - TELEBRAS, Núcleo de Segurança da Informação e Comunicações da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão, dentre outras. Porém, ao adotar o padrão *Common Criteria* (CC) na especificação dos serviços para a APF o Órgão Regulador C está estabelecendo um critério de certificação para esse tipo de produto.

Os Requisitos de Segurança de programas e equipamentos de TIC's para a APF incluem os Requisitos Funcionais de Segurança e os Requisitos de Garantia da Segurança, os quais estão alinhados à Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Os Requisitos Funcionais de Segurança contribuem com o desenvolvimento de produtos mais confiáveis buscando a prevenção de ameaças que possam existir em um ambiente operacional. Já os Requisitos de Garantia da Segurança buscam atender aos objetivos de segurança que foram estabelecidos, apresentando funcionalidades adequadas e com a devida implementação através da realização de avaliações. As avaliações incluem itens como por exemplo, Criticidade; Mitigação; Risco e Auditabilidade; Segurança; Testes de Segurança, etc. Os Órgãos da APF buscam celebrar contratos os quais permitam a auditabilidade do código fonte em situações que possam comprometer a segurança nacional de acordo com o Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos (2015).

Abaixo são definidos alguns dos requisitos específicos de Avaliação de Conformidade (RAC) para os serviços de Correio Eletrônico e VoIP. Os requisitos definidos abaixo não são exaustivos e encontram-se em uma versão inicial do processo de desenvolvimento e atualização pelo Programa Nacional de Homologação e Certificação de Ativos de TICs, desenvolvido pelo Órgão Regulador C, devendo evoluir conforme trabalhos do próprio Órgão Regulador C. Algumas considerações de segurança devem ser incluídas no processo de contratação do serviço de correio eletrônico na modalidade de serviço em nuvem, como, por exemplo, Mapeamento dos Riscos; Estrutura de Governaça entre cliente e fornecedor; Métricas de desempenho; Avaliações de vulnerabilidades; Mapeamento dos ativos; Gerenciamento dos riscos da informação; Segurança da cadeia de suprimento; Plano de recuperação de desastres; Portabilidade e Interoperabilidade dos dados; Guarda e recuperação de dados e Auditoria.

Os requisitos específicos de Avaliação de Conformidade RACs para o serviço de Correio Eletrônico incluem (1) Estrutura de Rede Segura e (2) Segurança de Servidores de E-mail. A Estrutura de Rede Segura deverá incluir itens de Localização da rede; Configuração de *Firewall*, Sistemas de Detecção de Intrusão (IDS) e *Switches* de rede. Para os Servidores de E-mail deverão incluir itens de Configuração, proteção e logs de arquivos, *Backup* de dados, proteção contra *malware*, testes de segurança e rastreabilidade remota.

Os RACs iniciais para o serviço de VoIP incluem (1) Estrutura de Rede Segura e (2) Práticas de segurança e controles para operação e manutenção. A Estrutura de Rede Segura prevê a separação lógica do tráfego de dados e voz conforme a norma BCP 5 RFC 1918 (1996). Deve-se utilizar mecanismos e protocolos seguros para todos os acessos de gerenciamento e auditoria aos ativos que integram o ambiente VoIP, além da utilização de mecanismos de criptografia para proteção das ligações e mecanismos de monitoramento de rede. Além disso, deve-se incluir alternativas para controle de falhas de energia elétrica visando manter os ativos do serviço de VoIP disponíveis. A qualidade deverá ser considerada no projeto do ambiente VoIP assegurando um nível que possa evitar problemas como *delay* (atraso), *jitter* (variação de atraso) e perda de pacotes.

As práticas de Gerenciamento de Segurança e Controle durante a Operação e Manutenção do Serviço VoIP devem incluir, mas não se restringirem aos seguintes itens: Política de segurança da informação específica; Tratamento de Riscos; Registro para cancelamento e revogação de usuários; Política de cópia de segurança; Plano de continuidade e contingenciamento do serviço de VoIP, Mecanismos para autenticação de

usuários; Atualização de manuais e Inventário dos ativos específicos para o serviço de telefonia, dentre outros. Além disso, as atualizações dos ativos do ambiente VoIP deverão ser testados antecipadamente em ambiente de homologação para posteriormente serem aplicados ao ambiente de produção.

A criticidade de um serviço do Órgão Regulador C vai depender das características especiais de alguns serviços de TI e será avaliada considerando o somatório de valores de criticidade do produto/serviço em cada dimensão, como por exemplo, grau de uso externo do produto, grau de dependência para continuidade do serviço público, tipo de operador do serviço, grau de classificação dos dados operados pelo serviço e tipo de uso de criptografia do produto. Para a avaliação da criticidade de um produto são definidos Níveis de Avaliação de Garantia (NAG) adequados à criticidade do produto, incluindo desde verificações básicas N0 às mais profundas, nível N3.

O Órgão Regulador C incentiva a criação de parceria público-privada para realização dos testes nos serviços de TIC's para a APF. Além disso, estimula a criação de uma Entidade ou órgão para certificar empresas a prestarem serviços que possam comprometer a segurança nacional, o que requer equipe técnica especializada.

Nos quadros a seguir serão exibidos os dados da coleta dos Formulários de Análise do Processo de Homologação e Certificação do produto nos Órgãos Reguladores A, B e C. Devido ao Órgão Regulador C encontrar-se em processo de desenvolvimento e atualização do Programa Nacional de Homologação e Certificação de Ativos de TICs, não apresenta dados para o formulário de certificação, apenas homologação. Por último serão exibidos os dados do Formulário de Análise baseado na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) para os Órgãos Reguladores A, B e C.

Quadro 4 - Itens do Formulário de Homologação em Órgãos Reguladores

Itens do Formulário de Análise do Processo de Homologação do Produto em Órgãos Reguladores			
ITENS	**Órgão Regulador A (Produto)**	**Órgão Regulador B (Produto)**	**Órgão Regulador C (Serviços)**
1. Protótipo	Amostra do produto com base na Resolução nº 506, de 1 de julho de 2008	Amostras do MCT operacionais e não operacionais Material de apoio (cartão, leitora, token) MCT 7 Vol I	Não observado
2. Carregamento e Teste do *Software*	Recomenda ao Fabricante RES 442 e 529	Recomenda ao Fabricante no MCT 7 Vol II	Parceria Público-Privado
3. Configurações no *Hardware*	Recomenda ao Fabricante RES 506	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135
4. Características de *Hardware*	Recomenda ao Fabricante RES 506	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135
5. Integração do *Software* ao *Hardware*	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135
6. Especificação dos Componentes Mecânicos e Interfaces Elétrica/Eletrônica	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135
7. Procedimentos de montagem e manufatura dos Componentes Mecânicos	Não observado	Não observado	Não se aplica
8. Procedimentos de montagem e manufatura dos Componentes Eletrônicos	Não observado	Não observado	Não se aplica
9. Procedimentos de revisão dos Componentes Mecânicos (listas de peças e componentes de cada parte, subsistema, e submontagem do produto)	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Não se aplica
10. Procedimentos de revisão dos Componentes Eletrônicos (listas de componentes eletrônicos, de gerbers para fabricação das peças, procedimentos de montagem eletrônica e revisão da documentação de teste da eletrônica)	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Não se aplica

Itens do Formulário de Análise do Processo de Homologação do Produto em Órgãos Reguladores			
ITENS	**Órgão Regulador A (Produto)**	**Órgão Regulador B (Produto)**	**Órgão Regulador C (Serviços)**
11. Falhas do Produto	Recomenda ao Fabricante na RES 529 e RES 442 Choque elétrico Aquecimento excessivo	Recomenda ao Fabricante FIPS 140-2 (*) Auto-Testes Energização e Condicionais -Proteção contra Falhas de Energia e Comunicação.	Recomenda os itens: VoIP:Energia secundária Alimentação secundária Fonte redundante Circuitos elétricos distintos Nobreaks, Descargas elétricas
12. Recursos de Produção do Produto	Não observado	Não observado	Não observado
13. Fornecedores	Não observado	Não observado	Múltiplas Entidades: SERPRO, DATAPREV, TELEBRAS, SLTI/MP
14. Instalação e configuração do *Software*	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135
15. Criticidade do *Software*_IEEE 1012	Não observado	Não observado	Somatório de valores de criticidade do produto/serviço
16. Validação e verificação do *Software*_IEEE 1012	Não observado	Não observado	Não observado
17. Desenvolvimento do *Software*_IEEE 1012	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Recomenda no DOC GT8135 Exceto (5) Testes Parceria Público-Privado
18. Testes_IEEE 1012	Recomenda ao Fabricante Compatibilidade Eletromagnética na (Resol. 442, 21.07.2006) Segurança Elétrica na (Resolução 529, 3.06.2009)	Recomenda ao Fabricante na FIPS 140-2	Parceria Público-Privado Correio Eletrônico: Testes de invasão, segurança (Ciclo de vida e ambiente de operação)
19. Documentação dos Testes_IEEE 1012	Não observado	Recomenda ao Fabricante no MCT 7 Vol II	Parceria Público-Privado
20. Impactos de mudanças no *Software*_IEEE 1012	Não observado	Não observado	Não observado
21. Alterações de Projeto	Não observado	Não observado	Recomenda no DOC GT8135

Itens do Formulário de Análise do Processo de Homologação do Produto em Órgãos Reguladores			
ITENS	**Órgão Regulador A (Produto)**	**Órgão Regulador B (Produto)**	**Órgão Regulador C (Serviços)**
22. Controle da Qualidade	Recomenda ao Fabricante na RES 242	Recomenda ao Fabricante na Portaria 8 de 8 de janeiro de 2013	Recomenda no DOC GT8135 VoIP: Nível de qualidade e desempenho da rede para evitar problemas de atraso (delay) e Jitter (variação de atraso).
23. Conclusão da Homologação	Certificado de Homologação	Certificado de Conformidade	Em elaboração pelo órgão C
24. Documentos de Homologação	Recomenda ao Fabricante	Recomenda ao Fabricante NSH1, NSH2 ou NSH3	Em elaboração pelo órgão C

Fonte: Elaborado pelo autor.

Quadro 5 - Itens do Formulário de Certificação em Órgãos Reguladores

Itens do Formulário de Análise do Processo de Certificação do Produto em Órgãos Reguladores		
ITENS	**Órgão Regulador A**	**Órgão Regulador B**
1. Planejamento da Certificação	- Certificado de Conformidade (comercializar) ou Declaração de Conformidade (uso próprio) - Recolhimento de emolumentos - Manual do usuário do produto - Informações cadastrais - Comprovação regular às leis brasileiras	- Certificado de Conformidade ou Laudo de Conformidade - Termo de Propriedade Intelectual - DOC Comprobatórios da representação regular; - Termo de Sigilo
2. Documentos para Planejamento da Certificação	O fabricante deverá apresentar um dos DOCs: -Declaração de conformidade - Declaração de conformidade com relatório de ensaio - Certificado de conformidade baseado em ensaio de tipo (CAT III) - Certificado de conformidade baseado em ensaio de tipo e em avaliações periódicas do produto (CAT II) ou - Certificado de conformidade com avaliação do sistema da qualidade. (CAT I)	O fabricante deverá apresentar ao OCP: -Solicitação formal; - NSC do Equipamento; - Documentação descrita no RGCP -Dados do fabricante
3. Documentação do Produto para Órgãos Certificadores	-Normas técnicas nacionais ou internacionais; - Regulamentos aplicáveis ao produto em outros países ou regiões; - Regulamentos editados pelo órgão regulador A; - Especificações do fabricante.	- Manuais do Produto e Níveis de Homologação; - Documentação Técnica: - Guia do Administrador; - Guia do Usuário.
4. Conformidade do Produto aos Requisitos Normativos	Certificado de Conformidade ou Declaração de Conformidade	Certificado de Conformidade ou Laudo de Conformidade
5. Testes (Tipo e Local)	Ensaios em laboratórios com *Software* fornecido pelo fabricante; Teste em campo do produto: Compatibilidade Eletromagnética (Resol. 442, 21.07.2006) Segurança Elétrica (Resolução 529, 03.06.2009)	Ensaios no LEA FIPS 140-2 MCT7-Vol I e II Auto-Testes: Energização e Condicionais.
6. Certificação do Produto	Certificado de Homologação	Ato Declaratório Selo de Homologação

Fonte: Elaborado pelo autor.

Quadro 6 - Itens do Formulário da Norma ISO/IEC_15408 em Órgãos Reguladores

Itens do Formulário de Análise baseada na Norma ISO/IEC_15408 (CC) em Órgãos Reguladores			
ITENS	**Órgão Regulador A**	**Órgão Regulador B**	**Órgão Regulador C**
1. Protection Profile (PP): (1) PP Introduction; (2) Conformance Claims; (3) Security Problem Definition; (4) Security Objectives; (5) Extended Components Definition e(6) Security Requirements.	Recomenda ao Fabricante (1) (2) (3) (6)	Recomenda ao Fabricante FIPS 140-2 ISO/IEC 15408	ISO/IEC 15408
2. Documentação para o Desenvolvimento do Produto: (1) Security Architecture; (2) Functional specification; (3) Implementation representation; (4) TSF internals; (5) Security policy modelling; e (6) TOE design: Descreve o projeto do TOE.	Não observado	Recomenda ao Fabricante FIPS 140-2 ISO/IEC 15408	ISO/IEC 15408
3. Documentação para o Usuário Final (1) Operational user guidance e (2) Preparative procedures	Recomenda ao Fabricante	Recomenda ao Fabricante FIPS 140-2 ISO/IEC 15408	ISO/IEC 15408
4. Controles de Desenvolvimento e Manutenção do Produto (1) CM capabilities; (2) CM scope; (3) Delivery; (4) Development security; (5) Flaw remediation; (6) Life-cycle definition e (7) Tools and techniques.	Não observado	Recomenda ao Fabricante FIPS 140-2 ISO/IEC 15408	ISO/IEC 15408
5. Segurança (1) ST Introduction; (2) Conformance claims; (3) Security problem definition; (4) Security objectives; (5) Extended components definition; (6) Security requirements e (7) TOE summary specification.	Recomenda ao Fabricante (6) Requisitos de segurança e não agressão ao ambiente	Recomenda ao Fabricante FIPS 140-2 ISO/IEC 15408	ISO/IEC 15408 Correio Eletrônico: Riscos, guarda e recuperação de dados, violação de dados.
6. Testes (1) Testes de cobertura; (2) Testes de profundidade (Depth Tests); (3) Testes independentes (Independent Tests) e (4) Testes funcionais (Functional Tests).	Recomenda ao Fabricante Compatibilidade Eletromagnética (RES 442) e Segurança Elétrica (RES 529)	Recomenda ao Fabricante na FIPS 140-2 no MCT7 Vol I (*)Auto-Testes: Energização e Condicionais	Parceria Público Privado CorreioEletrônico: segurança e rastreabilidade remota e testes de invasão
7. Análise de Vulnerabilidades (1) Vulnerability Survey; (2) Vulnerability Analysis; (3) Focused Vulnerability Analysis; (4) Methodical Vulnerability Analysis; (5) Advanced Vulnerability Analysis.	Não observado	Recomenda ao Fabricante na FIPS 140-2 NSF1 e NSF2 (**) Proteção contra ataques não invasivos.	Parceria Público Privado

Itens do Formulário de Análise baseada na Norma ISO/IEC_15408 (CC) em Órgãos Reguladores			
ITENS	**Órgão Regulador A**	**Órgão Regulador B**	**Órgão Regulador C**
8. Níveis de garantia de Avaliação do Produto EAL1, EAL2, EAL3, EAL4, EAL5, EAL6 e EAL7	Não observado	NSC1, NSC2 e NSC3	N0,N1,N2 e N3

Fonte: Elaborado pelo autor.

(*) Um módulo criptográfico deve realizar auto-testes na hora de ligar o módulo para assegurar que está funcionando corretamente. Se um auto-teste falhar, o módulo criptográfico estará comprometido e não pode ser mais considerado confiável.

(**) É recomendável que os MSC possuam proteções contra ataques não invasivos, como por exemplo, ataques por meio de emanações eletromagnéticas (EMA).

4.6 ANÁLISE DOS CASOS ESTUDADOS

Os estudos de casos deste trabalho, considerando os órgãos públicos, apresentam critérios distintos em relação ao processo de homologação e certificação de produtos. Entretanto, considerando as empresas privadas, apresentam procedimentos semelhantes para homologar e certificar seus produtos. Além disso, as práticas de segurança adotadas pelas empresas/órgãos dos estudos de casos, em sua grande maioria, refletem boa parte dos requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

A seguir, apresenta-se uma síntese comparativa dos casos analisados, considerando como base os itens presentes nos formulários aplicados (no caso das empresas privadas) e os critérios específicos adotados pelos órgãos públicos no processo de homologação e certificação.

Os órgãos públicos analisados neste estudo apresentam procedimentos sistematizados para a homologação e certificação de produtos de natureza cibernética. Nos Órgãos B e C algumas atividades do processo de homologação são recomendadas ao fabricante, como por exemplo, protótipos, especificação de componentes, validação do *software*, testes, etc. No caso o órgão B recomenda ao fabricante a utilização do padrão FIPS-1402 (NIST, 2001) para a realização dos testes e a utilização de três níveis para homologação do produto.

Em relação às atividades de certificação do produto, os órgãos reguladores A e B apresentam procedimentos semelhantes. O Órgão Regulador A possui regulamento específico para homologar e certificar os produtos que regula, conforme a Resolução nº 242/00 da Anatel. No caso do Órgão Regulador B, os critérios para homologação e certificação consolidam as políticas estabelecidas pela Infraestrutura de Chaves Públicas Brasileira do ICP-Brasil (2012). Entretanto, o Órgão Regulador C encontra-se em processo de desenvolvimento e atualização do Programa Nacional de Homologação e Certificação de Ativos de TIC’s e apesar de não possuir propósito de um processo de certificação, devido à seus serviços/produtos demandarem avaliação de outras entidades; ao adotar o padrão *Common Criteria* (CC) na especificação dos serviços para a APF o Órgão C está emitindo um requisito de certificação para esse tipo de produto.

No Órgão Regulador A existem duas formas para homologar produtos, a “Homologação por Certificação de Conformidade” com fins de comercialização do produto e a “Homologação por Declaração de Conformidade” para uso próprio. No Órgão

Regulador B é utilizado o processo de avaliação da conformidade no Programa de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil e deve-se observar os padrões e procedimentos técnicos propostos para verificar a conformidade do produto. No caso do Órgão Regulador B, os laboratórios acreditados emitem o "Certificado de Conformidade" na homologação de equipamentos (*Hardware*), e no caso dos sistemas (*Software*) emitem o "Laudo de Conformidade".

O processo de certificação é finalizado no Órgão Regulador A após análise pelo OCD e emissão do "Certificado de Conformidade", realizando o devido cadastro no SGCH do próprio órgão e emissão por este do "Certificado de Homologação", o qual autoriza o uso do selo para comercialização do produto. No caso do Órgão Regulador B, ocorre de forma semelhante, o mesmo recebe o "Certificado de Conformidade" enviado pelo OCP e após análise, sendo o parecer favorável, receberá autorização para utilização do Selo de Homologação e do correspondente número de identificação do equipamento.

Observou-se que os Órgãos Reguladores B e C utilizam os requisitos previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). No caso do órgão C, verificou-se uma maior cobertura das classes, devido à grande necessidade de segurança na prestação do serviço público ao cidadão, assim como aos riscos que os problemas de segurança possam impactar na Disponibilidade, Integridade, Confidencialidade e Autenticidade. Observou-se que o Órgão Regulador B prevê em sua documentação alguns dos itens previstos na referida norma como, por exemplo, documentos do Perfil de Proteção (PP): Especificação, Segurança, Interoperabilidade e Requisitos Funcionais. Também foi observado a adesão à classe Documentação e Gerenciamento citado na classe Suporte ao Ciclo de Vida do Produto. Além disso, o Órgão Regulador B adota requisitos de segurança derivados do padrão americano FIPS 140-2 (NIST, 2001), semelhante à família para requisitos de segurança estendidos previstos para a classe Perfil de Proteção (PP), além de realizar análise de vulnerabilidades através dos requisitos para Mitigação de outros ataques. Devido à complexidade do produto cibernético, o Órgão Regulador B prevê itens de gerenciamento, operacionalidade, restrição à substâncias nocivas e obrigatoriedade com alguns algoritmos criptográficos (Manual de Condutas Técnicas 7, v. 2.). Os testes realizados são bem específicos e incluem além dos previstos na FIPS 140-2 (NIST, 2001), energização e condicionais. Em relação aos níveis de garantia de avaliação do produto

(EAL1 a EAL7) previstos na Norma ISO/IEC-15408 (COMMON CRITERIA, 2012), o Órgão Regulador B adota três níveis de certificação: NSC1, NSC2 e NSC3.

No caso do Órgão Regulador A foi observado um pequeno escopo para cobertura dos requisitos previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), como por exemplo, *Protection Profile*(PP), documentação para o usuário, segurança e testes. Outros itens ficam a cargo do fabricante do produto, como, por exemplo, documentação e controles para o desenvolvimento do produto, análise de vulnerabilidades e níveis de garantia para avaliação do produto, concluindo que o referido órgão não suporta a Norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

Considerando as empresas privadas analisadas neste estudo, verificou-se que a Empresa A apresenta procedimentos bem definidos para o processo de homologação do produto, desde a definição de protótipos até a documentação para homologação, com exceção apenas de procedimentos para os componentes mecânicos. Apesar da Empresa B não ser fabricante do produto realiza diversas atividades para prestação do serviço cibernético de rastreamento veicular. A Empresa B recebe o produto diretamente do fabricante, ou seja, o produto já passou por todo o ciclo de desenvolvimento, porém necessita de algumas configurações iniciais realizadas no *Hardware* para o funcionamento do *Software*.

As Empresas A e B não apresentam procedimentos para os componentes mecânicos do produto, porém para os componentes eletrônicos a Empresa A possui documentação para aquisição, já na Empresa B existem apenas os procedimentos de montagem do produto no veículo incluindo testes da parte eletrônica. Para identificação de falhas potenciais no produto a Empresa A realiza testes de homologação, porém no caso da Empresa B não foram informados os procedimentos realizados em falhas na comunicação GPS/GPRS. Alguns componentes do produto da Empresa A são adquiridos de fornecedores, enquanto na Empresa B todo o produto é fornecido diretamente pelo fornecedor. As empresas realizam um *checklist* sobre os lotes dos componentes enviados pelos fornecedores para aprovar ou reprovar a peça.

Apenas a Empresa A possui atividades relacionadas à validação e verificação do *Software*, o qual é submetido à Comissão de Avaliação de Mudanças e Comissão de Avaliação de Revisão, que são áreas internas à empresa. No caso a Empresa B possui apenas uma Ficha de Mudanças para sugestões de melhorias no produto a serem enviadas

ao fabricante. As empresas A e B oferecem suporte técnico ao usuário. No caso da Empresa A são fornecidos ainda treinamentos *online* para certificação em seus produtos. As falhas identificadas no produto são tratadas de forma distinta pelas empresas privadas, sendo adotada uma série de procedimentos pela Empresa A desde documentação para registro das falhas, análises de risco e apoio da Comissão de Avaliação de Mudanças. No caso da Empresa B, por não ser fabricante do produto, a mesma gera uma nota de devolução que é encaminhada ao fabricante.

As Empresas A e B executam procedimentos semelhantes para verificação da qualidade do produto. A Empresa A possui um caderno de testes e realiza um comparativo com o número de defeitos encontrados no produto. No caso da Empresa B a qualidade é medida através do número de veículos localizados pelo Sistema de Monitoramento, assim como na eficácia das funções executadas pelo mesmo, como, por exemplo, bloqueio, alarme, etc. As empresas apresentam procedimentos semelhantes para conclusão da homologação do produto, no caso da Empresa A ocorre após a validação e aprovação de todas as funcionalidades do produto, sendo todas as atividades registradas em documentação específica. Por outro lado, na Empresa B ocorre após a execução de três procedimentos: configuração de parâmetros no produto, submissão do produto à bancada de testes e posterior aprovação dos testes realizados, porém não há registros de documentação.

Em relação ao processo de certificação do produto as empresas privadas analisadas apresentam procedimentos semelhantes. A certificação na Empresa A segue a Metodologia de Avaliação da CERTICS para *Software* (CTI ARCHER, 2013) e a estrutura do modelo segue os requisitos previstos na Norma ISO/IEC 15504-2 (ABNT, 2008). No caso da Empresa B existem três órgãos envolvidos no processo: a Anatel é responsável pela homologação das operadoras de telecomunicações na prestação dos serviços de telecomunicações e pelo Módulo de Comunicação Bi-direcional do produto, a Cesvi Brasil pela certificação nos sistemas de segurança do veículo como os rastreadores e devido a Empresa B ser prestadora de serviço de monitoramento e comunicação deverá ser certificada por um terceiro órgão, o Denatran.

Nas empresas privadas do estudo foram observadas algumas diferenças entre as mesmas na utilização dos requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). A Empresa A desenvolve a parte do *Software* do produto

cibernético e importa alguns componentes do *hardware*, utiliza documentação para descrever o produto, incluindo alguns dos itens previstos no Perfil de Proteção (PP) da Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), como, por exemplo, documentação de requisitos, segurança, RFC-2547 (SEMERIA, 2001), análise da segurança do código.

Entretanto, a Empresa B não apresenta documentação para o desenvolvimento do produto, devido a mesma não ser fabricante do mesmo. Em relação à documentação para o usuário final, a Empresa B não fornece, pois uma vez instalado no veículo, o usuário não tem contato com o mesmo, somente através do Sistema de Monitoramento. A Empresa B possui apenas o Manual de Instalação, voltado para os técnicos habilitados incluindo um *Checklist*. Já a Empresa A adota grande parte da documentação prevista na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), com exceção do Modelo Formal da Política de Segurança do produto.

As empresas A e B apresentam em suas instalações laboratórios para realização de testes no produto. Na Empresa A os testes são realizados pelo Departamento de Serviços Avançados e incluem diversos tipos como, por exemplo, independentes, de regressão, funcionais e não funcionais, de aceitação do usuário, carga, performance, stress e confirmação. Já na Empresa B o laboratório realiza testes nos componentes fornecidos pelo fabricante do produto e no *Software* de monitoramento. Porém não há informações de realização de testes para análise de vulnerabilidades no *Software* de monitoramento. No caso da Empresa A é utilizada uma ferramenta automatizada para realização de análise de vulnerabilidades do produto.

5 CONCLUSÕES E TRABALHOS FUTUROS

Neste capítulo são apresentados os resultados deste trabalho, ou seja, as conclusões obtidas a partir das análises desenvolvidas. Inicialmente são apresentadas as respostas às três questões básicas do objetivo geral da pesquisa e posteriormente são apresentadas as considerações finais do trabalho e direções de pesquisas futuras.

Tendo em vista o delineamento da pesquisa através das etapas planejadas na metodologia, o objetivo da pesquisa e seu desmembramento nas perguntas constituíram o alvo das reflexões e questionamentos do pesquisador.

Os resultados dos estudos de casos demonstraram que a metodologia utilizada conforme descrita no capítulo 3 permitiu identificar a sistemática de homologação e certificação utilizadas pelas empresas privadas e órgãos públicos pesquisados. Além disso, possibilitou a identificação de requisitos de segurança necessários aos produtos cibernéticos em estudo, assim como possibilitou conhecer algumas das características aplicáveis aos serviços de TIC's para a APF como, por exemplo, o correio eletrônico e VoIP. O desdobramento do objetivo nas perguntas da pesquisa facilita o entendimento, além de delimitar o escopo do trabalho.

As perguntas definidas para esta pesquisa foram: Q1) Que adaptações seriam necessárias ao MRM para que possa ser aplicado em empresas cujos produtos são cibernéticos? Q2) Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho ? Q3) Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho ? As questões de pesquisa foram respondidas da seguinte forma:

Q1) Que adaptações seriam necessárias ao MRM para que possa ser aplicado em empresas cujos produtos são cibernéticos? Segundo Wiener (1984), os produtos mecatrônicos são considerados essencialmente cibernéticos, uma vez que a ciência da cibernética é considerada como ciência da comunicação e controle. Diante deste fato tornou-se viável a utilização do MRM desenvolvido por Barbalho (2006) complementado por requisitos do *Common Criteria* (ISO/IEC_15480) e da Norma IEEE 1012-2012 na realização do diagnóstico da sistemática de homologação e certificação dos produtos cibernéticos. Além disso, a compilação dos dados coletados nos casos estudados através da

aplicação dos formulários (APÊNDICES A, B, C e D) contribuiram para identificar as práticas utilizadas pelas empresas e Órgãos públicos no processo de homologação e certificação de produtos.

Verificou-se que o MRM proposto por Barbalho (2006) poderia ser adaptado para ser utilizado em produtos cibernéticos. Na análise do processo de homologação foi necessário incluir questionamentos mais específicos em relação ao *Software*, como, por exemplo, as características para que o *Hardware* funcione com o mesmo, pois muitos produtos cibernéticos, principalmente os de infraestrutura críticas requerem uma grande quantidade de *Hardware* para o seu funcionamento. Além disso, foi utilizado perguntas mais específicas quanto ao processo de validação e verificação do *Software* conforme a Norma IEEE 1012-2012, complementando o MRM para obter maiores informações do funcionamento do produto cibernético em estudo.

O MRM com as adaptações citadas acima poderá ser aplicado para homologar e certificar produtos cibernéticos em empresas que desenvolvem tais produtos. Essas adaptações podem preencher de forma não absoluta a lacuna identificada na bibliografia pesquisada: a inexistência de uma padronização para homologar e certificar produtos cibernéticos que possibilite às empresas desenvolverem produtos mais confiáveis sob o aspecto da cibernética.

Q2) Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho ? Trata-se de uma questão extremamente ampla, cuja resposta completa necessitaria de um levantamento completo de todos os órgãos públicos envolvidos com o processo de certificação de produtos cibernéticos. Entretanto, este trabalho apresentou o estudo realizado em três órgãos públicos descritos nos estudos de caso. Nos órgãos reguladores observou-se que algumas recomendações ao fabricante estavam descritas em documentação específica de cada órgão, como por exemplo, em resoluções, manuais, etc. O órgão Regulador B obteve maior cobertura quanto aos itens de homologação do produto, apenas os procedimentos de montagem e manufatura dos componentes mecânicos e eletrônicos, recursos de produção do produto, fornecedores e alguns itens da Norma IEEE 1012-2012 não foram contemplados. No caso do órgão A não foi verificado procedimentos para integração do *software* ao *hardware*, especificação dos componentes mecânicos, procedimentos de montagem e manufatura dos componentes mecânicos e eletrônicos, além dos itens não

contemplados pelo Órgão Regulador B, porém obaservou-se que o órgão recomenda ao fabricante outros itens conforme exibido no Quadro 4. Por último, observou-se que Órgão C contempla a grande maioria dos itens do Formulário de Homologação, porém outros itens não são contemplados ou não se aplicam às caracteristicas do serviço desenvolvido pelo Órgão C, como por exemplo os itens (1,7,8,9,10,12,16,20) enquanto outros (23 e 24) estão em processo de elaboração pelo referido órgão.

Observou-se nos órgãos em estudo a adoção de legislação específica e regulamentos que direcionam o processo de homologação e certificação, além de possuírem documentação específica para o produto em estudo. Compilando-se os fluxos dos processos de homologação e certificação adotados pelos órgãos em estudo pode-se identificar grande semelhança entre os mesmos, com pequenas variações em relação às peculiaridades de cada produto e das entidades que acreditam os laboratórios como, por exemplo, no Órgão Regulador A alguns laboratórios são acreditados pelo Inmetro, porém existem Laboratórios de Ensaios Avaliados, ou seja, não acreditados pelo Innmetro, porém são avaliados conforme critérios estabelecidos pelo próprio Órgão Regulador A. Por outro lado, no Órgão Regulador B os laboratórios acreditados podem ser formados por entidade pública, privada ou mista, acreditada pelo Inmetro baseado em princípios e políticas adotadas no âmbito do Sistema Brasileiro de Avaliação da Conformidade - SBAC.

Os requisitos para homologação e certificação de produtos cibernéticos permitiram verificar que algumas atividades como os testes realizados pelos laboratórios acreditados, nem sempre eram conhecidos, dificultando a identificação das características do ambiente ao qual o produto é submetido. Além disso, algumas atividades inerentes à homologação são de responsabilidade do fabricante, principalmente as envolvidas no processo de desenvolvimento do produto, como, por exemplo, protótipo, arquitetura, definição de componentes, dentre outras.

Segundo Rozenfeld, 2006, caso seja exigida por órgão regulamentador a primeira certificação poderá ocorrer na fase de homologação do produto, o que pôde ser confirmado pelos Órgãos Reguladores A e B. Observou-se que os órgãos reguladores B e C adotam em grande parte os requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Além disso, os ativos de TI regulados pelo Órgão C são considerados estratégicos e em determinadas situações vitais para a segurança do Estado, o que leva à necessidade de adoção de práticas de segurança que incluam a realização de auditorias em

seus programas e equipamentos. Devido a este fato, os RACs desenvolvidos para os serviços no Órgão Regulador C encontram-se alinhados à norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

Entende-se que os requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) são atendidos pelos Órgãos Reguladores B e C. Observou-se um escopo reduzido de adesão aos requisitos pelo Órgão A, concluindo que o mesmo não adota a referida Norma. Além disso, observou-se que os Órgãos reguladores incluem itens de segurança não só para o produto como também para o ambiente de operação do mesmo, como por exemplo, no Órgão Regulador A o produto em estudo não pode causar interferências em qualquer sistema operando em caráter primário, além de possuir restrições de faixa de frequências, intensidade de campo (Resolução nº 506/08 da Anatel) requisitos de segurança elétrica (Resolução nº 529/09 da Anatel) e de perturbações eletromagnéticas (Resolução nº 442/06 da Anatel). Já no Órgão B inclui itens de segurança física visando a proteção contra sondagem e violação direta além de restrições a substâncias nocivas. No caso do Órgão C, a segurança inclui mecanismos e protocolos seguros, fontes redundantes, energia secundária, proteção contra descargas elétricas, plano de continuidade e contigenciamento do serviço de VoIP, Riscos, etc.

Verificou-se ainda a utilização pelo Órgão Regulador B de requisitos estendidos de outra norma como, por exemplo, a FIPS PUB 140-2 (NIST, 2001), devido as características de segurança do produto em estudo. Os processos de homologação e certificação adotados pelos órgãos reguladores neste estudo mesmo considerando suas especificidades inerentes às características de cada produto cibernético, proporcionaram uma visão do entendimento do processo, dos requisitos do produto e das entidades envolvidas no mesmo.

Q3) Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho ? A resposta a esta questão se restringe às empresas privadas analisadas no estudo de caso nas quais foram identificadas várias atividades relacionadas ao processo de homologação e certificação de produtos cibernéticos. Porém, quando componentes do produto eram adquiridos de fornecedores, as atividades relacionadas com o ciclo de desenvolvimento do produto não eram conhecidas. Foi o caso observado na Empresa B, que apesar de não ser fornecedora, apresenta atividades reduzidas para homologação do produto, como por exemplo,

configurações no *hardware*, procedimentos de montagem de componentes do produto, controle da qualidade e testes de homologação.

Observou-se que a certificação do produto na Empresa A segue a Metodologia de Avaliação CERTICS para *Software* e apresenta procedimentos bem definidos em seus processos, além de possuir uma estrutura consolidada dentro da própria empresa para realização de testes que possibilitam simular o ambiente operacional. Porém, no caso da Empresa B o planejamento da certificação fica a cargo do fabricante, a empresa já recebe o produto certificado pelos órgãos competentes. Observou-se que apenas a Empresa A adota em sua grande maioria os requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Devido a Empresa B não ser fabricante do produto dificultou-se a identificação dos requisitos de segurança adotados pelo fabricante.

Assim, considera-se que a resposta para esta pergunta é diferenciada para as empresas, havendo conhecimento do cumprimento dos requisitos de homologação e certificação do produto desenvolvido, com maior cobertura, apenas pela Empresa A. Conclui-se que tal diferenciação é devida a uma série de fatores, dentre eles, o desconhecimento dos requisitos de segurança adotados pelo fabricante do produto da Empresa B, como, por exemplo, no item do tratamento das vulnerabilidades do *Software* de monitoramento veicular. No caso da Empresa A o próprio produto possibilita a adoção de estratégias preventivas contra ameaças cibernéticas.

O estudo permitiu identificar as lacunas existentes entre os requisitos de segurança relacionados à defesa cibernética e as práticas de homologação e certificação adotadas pelas Empresas/Órgãos. Além disso, alguns autores (SHAFQAT; MASSOD, 2016), reconhecem a lacuna existente na literatura da ausência de uma padronização em segurança cibernética. Através da pesquisa foi possível contribuir cientificamente para a elaboração de estratégias de certificação e homologação de produtos cibernéticos, tendo como base o MRM proposto por Barbalho (2006) com as devidas adptações sugeridas aos produtos cibernéticos. Além disso, a adoção de requisitos de segurança propostos pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) viabiliza o desenvolvimento de produtos cibernéticos com maior grau de confiabilidade.

Além das perguntas da pesquisa, outras considerações tornaram-se relevantes no decorrer do trabalho, como por exemplo, a necessidade de parceria entre as empresas públicas e privadas para realização dos testes nos serviços de TICs para a APF, além da

criação de uma entidade que certifique empresas a prestarem serviços que possam comprometer a segurança nacional, conforme constatado pela literatura no trabalho de Min, Chai e Han (2015). Observou-se que o Órgão Regulador C realiza também o papel de comprador, atuando diretamente no desenvolvimento dos serviços de TICs.

Outra característica observada no Órgão Regulador A, mostra que quando os produtos forem utilizados pelas Forças Armadas utilizando radiofrequências nas faixas destinadas a fins exclusivamente militares, serão dispensados de certificação ou homologação pelo Órgão Regulador A, devendo cumprir legislação específica para produtos de uso militar.

Uma das características observadas na pesquisa, mostra que a Empresa A, disponibiliza soluções de forma dual, ou seja, o mesmo produto utilizado para defesa cibernética é também comercializado nos mercados público e privado, o que possibilita à Empresa A uma maior aceitação dos seus produtos ao mercado. Observou-se que as Empresas A e B possuem atividades diferenciadas dentro da cadeia produtiva de produtos cibernéticos, como por exemplo, o controle de mudanças no *software*, testes, segurança, controle da qualidade, dentre outros.

Observou-se que o estudo baseado na Metodologia de Certificação para Equipamentos de TI proposta no trabalho de Coelho e Silva (2013) não é aplicável a todo e qualquer tipo de produto cibernético, como os serviços definidos pelo Órgão Regulador C. Porém, para os órgãos reguladores A e B os produtos possuem correspondência com a Subclasse A: Equipamento capaz de se conectar diretamente à rede.

Além disso, para o produto do Órgão Regulador A, devido as características do ambiente ao qual o produto será inserido com estações que operam em caráter secundário, não há como atender ao item referente ao isolamento da comunicação com o meio externo para realização dos testes em laboratório, previsto na referida metodologia. Já para o órgão Regulador B, os requisitos de segurança incluem proteção contra ataques não invasivos, como por exemplo, ataques por meio de emanações eletromagnéticas, contemplando o isolamento da comunicação, conforme previsto na referida metodologia. Os demais itens previstos na proposta de Coelho e Silva (2013) como por exemplo, classificação das entidades envolvidas, registro e identificação do equipamento, sistematização da ontologia, relatório técnico e certificação são contemplados pelos Órgãos reguladores A e B, porém os testes são específicos para os produtos dos órgãos A e B e nem sempre há

correspondência com os descritos na referida metodologia. Por último, em relação ao nível de garantia de precisão para eventos registrados, foi observado contemplação apenas pelo Órgão Regulador B, NSF1 e NSF2.

O modelo proposto por Barbalho (2006) inclui em sua fase de validação, além de itens pertinentes à certificação do produto, aborda a validação do produto com o cliente. Neste estudo não foram abordadas perguntas relativas a validação do produto, pois o objetivo deste trabalho se delimitou na realização do diagnóstico da sistemática de homologação e certificação de produtos cibernéticos. A implementação dos requisitos de segurança propostos pela norma ISO/IEC_15408 (COMMON CRITERIA, 2012) nas empresas dos estudos de caso, não é escopo deste trabalho. Nesse sentido, devido a apresentação de restrições de publicidade de informações internas consideradas por algumas empresas como sigilosas, muitas organizações não permitem uma intervenção mais profunda em seus processos. Portanto, embora não seja possível realizar de fato a implementação dos requisitos de segurança no processo de desenvolvimento do produto nas empresas deste estudo, foram fornecidas recomendações de melhorias e diretrizes para o desenvolvimento de tais produtos (especificamente no que tange à homologação e certificação) com base na realização do diagnóstico.

Como direções para pesquisas futuras sugere-se a definição dos testes específicos para validação dos requisitos dos ativos de TICs utilizados pela APF. Neste caso, sugere-se explorar os tipos de testes realizados pelos laboratórios acreditados, o que requer uma análise mais profunda e específica. Além disso, após a conclusão do Programa Nacional de Homologação e Certificação de Ativos de TICs, desenvolvido pelo Órgão Regulador C pode-se explorar os RACs dos outros serviços utilizados na APF. Além disso, pode-se adicionar perguntas ao Formulário de homologação do produto, envolvendo características mínimas do ambiente para o funcionamento do mesmo, pois alguns produtos, devido à sua complexidade podem exigir condições específicas do ambiente para sua operação, como foi demonstrado neste estudo. Outro ponto relevante a ser explorado, envolve a sugestão de adaptações que possam refletir melhor os produtos/serviços cibernéticos na Metodologia de Certificação para Equipamentos de TI proposta no trabalho de Coelho e Silva.

REFERÊNCIAS

ADAMOWSKI, J. C.; FURUKAWA, C. M. Mecatrônica: uma abordagem voltada à automação industrial. **Mecatrônica Atual**. São Paulo, n.1, p. 8-11, out. – nov., 2001.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. **Drones.** Disponível em: <http://www.anac.gov.br/assuntos/paginas-tematicas/drones>. Acesso em: 17 fev. 2017.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Ato nº 1135, de 18 de fevereiro de 2013.** [s. d.], [s. l.], 2013.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Instruções para homologar produtos por declaração de conformidade com relatório de ensaio** . Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=326454&pub=original&filtro=1&documentoPath=326454.pdf> .Acesso em: 02 out. 2015.

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL. **Sistemas aplicados a energia e meio ambiente.** Brasília: ABDI, 2010. (Cadernos Temáticos Tecnologias de Informação e Comunicação 5). Disponível em: <http://www.abdi.com.br/Estudo/Caderno%20Tem%C3%A1tico%20TIC%20-%205%20%20(Vers%C3%A3o%20Final)%20-%20Sistema%20Aplicados%20a%20Energia%20E%20meio%20Ambiente.pdf>. Acesso em: 06 ago. 2016

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Requisitos técnicos e procedimentos de ensaios aplicáveis à certificação de produtos para telecomunicação de categoria II**. 2016. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documentoVersionado.asp?numeroPublicacao=326624&documentoPath=326624.pdf&Pub=&URL=/Portal/verificaDocumentos/documento.asp> .Acesso em: 02 out. 2016.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 242, de 30 de novembro de 2000.** Aprova o Regulamento para Certificação e Homologação de Produtos para Telecomunicações. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/15-2000/129-resolucao-242>. Acesso em: 12 dez. 2016.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 442, de 21 de julho de 2006.** Aprova Regulamento para a Certificação de Equipamentos de Telecomunicações quanto aos Aspectos de Compatibilidade Eletromagnética. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2006/352-resolucao-442>. Acesso em: 14 dez. 2016

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 506, de 01 de julho de 2008.** Republica o Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.. Resolução Nº 506. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/23-2008/104-resolucao-506>. Acesso em: 12 dez. 2016

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 529, de 3 de junho de 2009.** Aprova o Regulamento para Certificação de Equipamentos de Telecomunicações quanto aos Aspectos de Segurança Elétrica. Disponível em: < http://www.anatel.gov.br/legislacao/resolucoes/2009/149-resolucao-529>. Acesso em: 15 dez. 2016.

AKER SECURITY SOLUTIONS. **Aker IPS:** manual. [s. l.]: [s. n.], 2016. 71 p. Disponível em: <http://download.aker.com.br/prod/current/manuais/aker-ips/aker-IPS-1.0.1-pt-manual-001.pdf>. Acesso em: 02 nov. 2016

AL-AHMAD, W. A detailed strategy for managing corporation cyber war security. **International Journal of Cyber-Security and Digital Forensics**, v.2, n. 4, p.1-9, 2013.

ALBERTS, Chris et al. **Defining incident management processes for CSIRTs**: a work in progress. Pittsburgh: Carnegie Mellon Software Engineering Institute, 2004. Disponível em: <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14405.pdf>. Acesso em: 19 out. 2016.

ALVAREZ CABRERA, A. A. et al. Towards automation of control software: A review of challenges in mechatronic design. **Mechatronics**, [s.l.], v. 20, n. 8, p.876-886, dez. 2010.

ALVES, A. M.; SALVIANO. C. F.; STEFANUTO, G. N. **Certificação CERTICS**: um instrumento de política pública para inovação tecnológica em software. Campinas, São Paulo, 2015.

ANJOS, E. G. P.. **A evolução da eletrônica embarcada na indústria automobilística brasileira.** 2011. 124 f. Monografia (Especialização) - Curso de Engenharia de Processos Industriais, Instituro Mauá de Tecnologia, São Caetano do Sul, 2011.

ASHLEY, S. Getting a hold on mechatronics. **Mechanical engineering,** v. 119, n. 5, p. 60-63, maio 1997.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 15504-2:** Tecnologia da informação: Avaliação de processo: Parte 2: Realização de uma avaliação. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17025:** Requisitos gerais para a competência de laboratórios de ensaio e calibração. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **O que é Certificação e como obtê-la?** Disponível em: <http://www.abnt.org.br/certificacao/o-que-e>. Acesso em: 29 nov. 2015.

BARBALHO, S. C. M. *et al*. **Fundamentos do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética (SHCDCiber).** Brasília: Universidade de Brasília, 2014.

BARBALHO, S. C. M. **Modelo de referência para o desenvolvimento de produtos mecatrônicos: proposta e aplicações**. Tese (Doutorado em Engenharia Mecânica) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2006.

BARNETT, Arnold. CAPPS II: The foundation of aviation security?. **Risk Analysis,** [s.l.], v. 24, n. 4, p.909-916, ago. 2004

BASKERVILLE, Richard L.; PORTOUGAL, Victor. A possibility theory framework for security evaluation in national infrastructure protection. **Journal Of Database Management**, [s.l.], v. 14, n. 2, p.1-13, 2003.

BHATTI, Babar. **Telematics in Pakistan**. 2009. Disponível em: <http://telecompk.net/2009/06/30/telematics-in-pakistan/>. Acesso em: 30 jul. 2016.

BERMAN, O.; DREZNER, Z.; WESOLOWSKY, G. O. Routing and location on a network with hazardous threats. **The Journal Of The Operational Research Society**, [s.l.], v. 51, n. 9, p.1093-1099, set. 2000.

BEST CURRENT PRACTICE. **BCP 5 RFC 1918:** Address allocation for private internets. 1996. Disponível em: <https://www.rfc-editor.org/rfc/pdfrfc/rfc1918.txt.pdf>. Acesso em: 25 nov. 2016.

BOCCARDO, D. R. et al. Modelo de segurança para ambientes de avaliação e testes de segurança de software. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 15., 2015, Florianópolis. **Anais...** . Florianópolis: Sociedade Brasileira de Computação, 2015. p. 501 – 509

BRADLEY, D. A. et al. .**Mechatronics:** electronics in products and processes . London: Chapman and Hall, 1991.

BRASIL. Ministério da Defesa. Portaria nº 3229, de 27 de novembro de 2013. Classifica Produtos Estratégicos de Defesa – PED. **Diário Oficial da União**. Disponível em: <http://www.defesa.gov.br/arquivos/industria_defesa/cmid/produtos_estrategicas_de_defesa.pdf>. Acesso em: 10 abr. 2015.

BRASIL. Ministério do Desenvolvimento, Indústria e Comércio Exterior. Instituto Nacional de Metrologia, Qualidade e Tecnologia. **Portaria nº 8, de 08 de janeiro de 2013.** Requisitos de avaliação da conformidade para equipamentos de certificação digital padrão ICP - Brasil. Disponível em: <http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001958.pdf> Acesso em: 15 nov. 2016

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Padrões de Interoperabilidade de Correio Eletrônico: documento de referência.** Brasília: Ministério do Planejamento, Orçamento e Gestão, 2016. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/e-PING_v2016_26022016.pdf/at_download/file> Acesso em: 12 set. 2016.

BRASIL. Presidência da República. Ministério do Planejamento, Orçamento e Gestão. **Conjunto de características, critérios, condições mínimas e medidas para auditoria de segurança da informação em programas e equipamentos.** Brasília: Ministério do Planejamento, Orçamento e Gestão, 2015. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/GT8135 - CriteriosAuditoriaSeguranca V 04_08_15.pdf>. Acesso em: 25 nov. 2016.

BRASIL. **Decreto nº 8135, de 04 de novembro de 2013**. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 25 nov. 2016.

BRASIL. Presidência da República. Ministério do Planejamento, Orçamento e Gestão. **Modelo de governança e gestão para a auditoria de segurança da informação em programas e equipamentos.** Brasília: Ministério do Planejamento, Orçamento e Gestão, 2015. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/GT8135%20-%20Modelo%20de%20Governanca%20de%20Auditoria%20V%2004_08_15.pdf> Acesso em: 25 nov. 2016.

BUUR, J; ANDREASEN, M. M. **A theoretical approach to mechatronical design.** Institute for Engineering Design. Lyngby: Technical University of Denmark, 1990..

CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS. **Eletrônica para automação:** relatório panorama setorial. Brasília: Centro de Gestão e Estudos Estratégicos, 2009. Disponível em: <http://www.abdi.com.br/Estudo/eletronica para automação.pdf>. Acesso em: 17 ago. 2015

CENTRO DE ESTUDOS, RESPOSTA, E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 15 set. 2015.

CENTRO DE EXPERIMENTAÇÃO E SEGURANÇA VIÁRIA. **Sobre nós.** Disponível em: <http://www.cesvibrasil.com.br/site.aspx/sobre-nos>. Acesso em: 17 fev. 2017.

CENTRO DE TECNOLOGIA DA INFORMAÇÃO RENATO ARCHER. **Metodologia de Avaliação da CERTICS para Software.** Campinas, 2013. Disponível em: <http://www.certics.cti.gov.br/downloads/Definicao_MetodologiaCERTICS.pdf>. Acesso em: 31 out. 2016.

CHENG, Yi et al. Integrated situational awareness for cyber attack detection, analysis, and mitigation. In: SENSORS AND SYSTEMS FOR SPACE APPLICATIONS, 5., 2012, Baltimore. **Proceedings...** . Baltimore: Spie, 2012.

CHIOCHETTAM, J. C., CASAGRANDE L. F.; ECHEVESTE M. E. Análise comparativa entre o modelo referencial de Rozenfeld e um processo de desenvolvimento de produto. **TECAP**, v. 2. 2, n. 2, p. 19-26, 2008.

CLARK, K. B.; FUJIMOTO, T. **Product development performance: strategy, organization and management in the world auto industry.** Boston: Harvard Business School Press, 1991.

COELHO, M. P.; SILVA, R. M. Trustiness certification of information technology equipment. **International Journal of Computer Science and Network Security**, v.13, n. 12, p.35-42, dez. 2013.

COMMON CRITERIA. **Common Criteria for information technology security evaluation:** part 3: Security assurance components. S. L, 2012. Disponível em: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf>. Acesso em: 04 jun. 2015.

COOPER, R. **Winning at New Product:** accelerating the process from idea to launch. Massachussetts: Addison-Wesley Publishing Company, 1993.

CROSBY, P. B. **Qualidade é investimento**. 7. ed. Rio de Janeiro: José Olympio, 1999.

DARAS, Nicholas J.. Stochastic analysis of cyber-attacks. **Applications of Mathematics and Informatics in Science and Engineering,** [s.l.], p.105-129, 2014

DEMO, P. **Pesquisa e construção de conhecimento.** Rio de Janeiro: Tempo Brasileiro, 1996.

DEPARTAMENTO NACIONAL DE TRÂNSITO. **Portaria nº 253, de 22 de julho de 2009**. Portaria Nº 253, de 22 de Julho de 2009. Disponível em: <http://www.denatran.gov. br/download/Portarias/2009/PORTARIA_DENATRAN_253_09.pdf>. Acesso em: 27 nov. 2016.

DORF, C. R.; BISHOP, R. H. **Sistemas de controle modernos.** Rio de Janeiro: LTC, 2002.

EISENHARDT, K. M. Building theories from case study research. **The Academy of Management Review,** v. 14, n. 4, p. 532-550, out.1989.

FERNANDES, J. H. C. **Segurança e defesa cibernética para reduzir vulnerabilidades nas infraestruturas críticas nacionais.** Brasília: Núcleo de Estudos Prospectivos da 7ª Subchefia do Estado Maior do Exército Brasileiro, 2012.

GIL, A. C. **Como elaborar projetos de pesquisa.** 5 ed. São Paulo: Atlas**,** 2010.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6.ed. São Paulo: Atlas, 2008.

HORIKAWA, O. **Características de projeto de sistemas mecatrônicos**. Tese (Livre Docência). São Paulo: Universidade de São Paulo, Escola Politécnica, 2000.

HUNT, V. D. **Mechatronics:** Japan's newest threat. New York: Chapman and Hall, 1988.

IEEE COMPUTER SOCIETY. **1012-2012:** IEEE standard for software verification and validation. 2012. Disponível em: <https://standards.ieee.org/findstds/standard/1012-2012.html>. Acesso em: 01 out. 2016.

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **DOC-ICP-10:** Regulamento para homologação de sistemas e equipamentos de certificação digital no Âmbito da ICP-Brasil. 2012. Disponível em: <http://www.iti.gov.br/images/legislacao /Docicp/DOC-ICP-10_-_Versao_3.0_Regulamento_para_Homologacao-1.pdf>. Acesso em: 19 out. 2016

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **DOC ICP-10.01:** Procedimentos administrativos para homologação na ICP-Brasil. 2015. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/docs13082012/DOC-ICP-10.01_-_Versão_3.3_-_PROCEDIMENTOS_ADMINISTRATIVOS_PARA_ HOMOLOGAÇÃO_NA_ICP-BRASIL.pdf>. Acesso em: 19 out. 2016.

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **DOC ICP-10.02:** Estrutura normativa técnica e níveis de segurança de ensaios para sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. 2010. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-10.02.pdf>. Acesso em: 19 out. 2016

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **DOC-ICP 10.05:** Padrões e procedimentos técnicos a serem observados nos processos de homologação de Módulos de Segurança Criptográfica (MSC) no âmbito da ICP-Brasil. 2007. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-10.05_-_v_1.0.pdf>. Acesso em: 20 out. 2016

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Manual de condutas técnicas 7, v. I**: Requisitos, materiais e documentos técnicos para homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICPBrasil. 2016. Disponível em: <http://www.iti.gov.br/images/servicos/homologacao/MCT-7__Vol.1_V_2.0_.pdf>. Acesso em: 21 out. 2016.

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Manual de condutas técnicas 7, v. II**: Procedimentos de ensaios para avaliação de conformidade aos requisitos

técnicos de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil. 2016. Disponível em: <http://www.iti.gov.br/images/servicos/homologacao/MCT-7__Vol.2_V_2.0_.pdf>. Acesso: em 21 out. 2016.

ISACA/RSA CONFERENCE, 2016. **State of cybersecurity:** implications for 2016. Rolling Meadows: Isaca, 2016. Disponível em: <http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf> Acesso em: 10 mar. 2016.

ISERMANN, R. **Mechatronic systems:** fundamentals. London: Springer Verlag, 2005.

KNAPP, Kenneth J.; BOULTON, William R.. Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. **Information Systems Management**, [s.l.], v. 23, n. 2, p.76-87, mar. 2006.

KRYPTUS. **AHX4 ASI-HSM:** o HSM padrão da ICP-Brasil. Disponível em: <https://www.kryptus.com/asi-hsm>. Acesso em: 12 nov. 2016.

KUO, B. C. **Automatic control systems**. 4 ed. Englewood Cliffs: Prentice Hall, 1982.

LONCHAMPT, P.; PRUDHOMME, G.; BRISSAUD, D.. Engineering design problem in a co-evolutionary model of the design process. In: INTERNATIONAL DESIGN CONFERENCE, 8., 2004, Dubrovnik. **Proceedings...** . Dubrovnik: Marjanovic D., 2004. p. 361 - 366.

MARTINS, Gilberto Andrade. Estudo de caso: uma reflexão sobre a aplicabilidade em pesquisa no Brasil. **Revista de Contabilidade e Organizações,** São Paulo, v. 2, n. 2, p. 9-18, apr. 2008.

MIGUEL, P. A. C. Estudo de caso na administração: estruturação e recomendações para sua condução. **Produção**, v. 17, n. 1, p. 216-229, 2007.

MIN, K.; CHAI. S.; HAN, M. An international comparative study on cyber security strategy. **International Journal of Security and Its Applications.** v. 9, n. 2, p. 13-20, 2015.

MINAYO, M. C. S. **Pesquisa social:** teoria, método e criatividade. Petrópolis: Vozes, 1994.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos** -

Fundamentos, Técnicas, Tecnologias, Estratégias. São Paulo/SP. Editora Novatec, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**. CPS Public Working Group**. 2016. Disponível em: <https://www.nist.gov/el/cyber-physical-systems/cps-public-working-group-pwg>. Acesso em: 12 ago. 2015.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **FIPS PUB 140-2:** Security requirements for cryptographic modules. 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Acesso em: 12 ago. 2016

OLIVEIRA, Malena. Empresas buscam antecipar tendências contra ciberataques. **Estadão: O Estado de S. Paulo.,** 23 fev. 2016. Disponível em: <http://economia.estadao.com.br/noticias/governanca,empresas-buscam-antecipar-tendencias-contra-ciberataques,10000017751>. Acesso em: 10 mar. 2016.

PAHL, G. et al. **Engineering design:** a systematic approach. 2. ed. London: Springer Verlag, 1996.

PARKS, R. C.; DUGGAN, D. P. Principles of cyber-warfare. **Workshop on Information Assurance and Security. IEEE**. p. 122-125, 2001.

Portal Brasil. **Força Aérea esclarece normas para voos de drones no Brasil**. 2015. Disponível em: <http://www.brasil.gov.br/defesa-e-seguranca/2015/03/forca-aerea-esclarece-normas-para-voos-de-drones-no-brasil>. Acesso em: 03 nov. 2015.

RAJKUMAR, Ragunathan. A Cyber-Physical Future. **Proceedings of the IEEE**, v. 100, p. 1309-1312, maio 2012. Disponível em: < http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6187688> Acesso em: 18 dez. 2015

ROSÁRIO, J. M. **Princípios de Mecatrônica.** São Paulo/SP: Editora Pearson, 2005.

ROZENFELD, H. **Gestão de Desenvolvimento de Produtos**. São Paulo/SP: Editora Saraiva, 2006.

SALMERON, J.; WOOD, K.; BALDICK, R. Analysis of electric grid security under terrorist threat, **IEEE Trans. Power Systems**. Vol. 19, n. 2, p. 905-912, 2004.

SAT AUTOMAÇÃO INDUSTRIAL. **A quarta revolução industrial pode impactar o crescimemto sustentável.** 2016. Disponível em: <http://www.satautomacao.com.br/noticias/370/A_quarta_revolucao_industrial_pode_impactar_o_crescimemto_sustentavel>. Acesso em: 12 nov. 2016.

SEMERIA, Chuck. **RFC 2547bis:** BGP/MPLS VPN Fundamentals. Sunnyvale: Juniper Networks, 2001. Disponível em: <https://pdfs.semanticscholar.org/d274/2676bc8c35b3e9700143d938ecf6f285a885.pdf>. Acesso em: 02 nov. 2015.

SELLTIZ, C.; JAHODA, M.; DEUTSCH, M. **Métodos de pesquisa nas relações sociais**. São Paulo: EDUSP, 1974.

SHAFQAT, N.; MASSOD, A. Comparative analysis of various national cyber security strategies. **International Journal of Computer Science and Information Security**. v. 14, n. 1, p. 129-136, 2016.

SHARMA, A. Cyber wars: paradigm shift from means to ends. **Strategic Analysis**, vol. 34, n.1, pp. 62-73, 2010.

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 3a ed. São Paulo: Pearson, 2010.

TANG, L. et al. Trustworthiness analysis of sensor data in cyber-physical systems. **Journal of Computer and System Sciences,** Estados Unidos, v. 70, p. 383-401, 2013.

TINNEL, L.; SAYDJARI, S.; FARELL, D. Cyberwar Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. **Workshop on Information Assurance**. **IEEE,** 2002.

ULRICH, K. T.; EPPINGER, S. D. **Product design and development**. New York: McGraw-Hill, 1995.

VARANDAS JUNIOR, A.; MIGUEL, P. A. C. Análise do processo de preparação da produção no desenvolvimento de novos produtos por meio de um estudo de caso em uma empresa do setor siderúrgico. **Produção** [online]. 2012, v. 22, n.2, p.185-200, 2012. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-65132012000200001&lng=en&nrm=iso> Acesso em: 18 ago. 2015.

WALDEN, J.; KAPLAN, H. Estimating time and size of bioterror attack. **Emerging Infectious Diseases**, vol. 10, n. 7, p. 1202-1205, 2004.

WEIN, L.; BAVEJA, M. M. Using fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program. **Proceedings Of The National Academy Of Science**, v. 102, n. 21, p.7772-7775, 13 maio 2005. Proceedings of the National Academy of Sciences.

WIENER, N. **Cibernética e sociedade:** o uso humano de seres humanos. 3.ed., São Paulo: Cultrix, 1968.

YIN, R. K. **Estudo de caso:** planejamento e métodos. 3 ed. Porto Alegre: Bookman, 2005.

APÊNDICE A– Formulário de análise do processo de homologação do produto

PRODUTO/SERVIÇO: <PRODUTO>	
RESPONSÁVEL:	
CARGO/FUNÇÃO:	
DATA: EMAL:	
ITEM	**ANÁLISE DO PROCESSO DE HOMOLOGAÇÃO**
001	A empresa utiliza protótipos para homologar os produtos?
EMPRESA	
MRM	Sim. Protótipos Beta (Protótipos completo do produto que serão utilizados para a otimização do produto).
002	Como são definidos os procedimentos necessários ao carregamento e teste do *software* desenvolvido ? São documentados ? Como?
EMPRESA	
MRM	É realizado o detalhamento da documentação necessária ao carregamento e teste do *software*. São documentados. Existe documentação de instalação/configuração de *software*, e carregamento e testes de *software*.
003	Há necessidade de ajuste/configuração do *hardware* para o funcionamento do *software* ?
EMPRESA	
MRM	Sim. Existe documentação de configuração do computador.
004	Há alguma característica de *hardware* sem a qual o *Software* não funciona?
EMPRESA	
MRM	Memória RAM, HD, Processador, Placa de Vídeo, etc.
005	Existem procedimentos de integração do *Software* ao *Hardware* ?
EMPRESA	
MRM	Sim. Existe documentação de testes de integração do *software* e *hardware*.
006	Como os componentes mecânicos do produto são especificados para aquisição, fabricação e montagem ? Existem interfaces com a parte ELÉTRICA/ELETRÔNICA ?
EMPRESA	
MRM	Através da definição dos materiais que serão processados e o detalhamento dos processos de fabricação e desenhos a serem utilizados, incluindo os componentes de cada parte, subsistema e submontagem do produto. Os materiais do produto podem ser divididos em: metálicos e não-metálicos.
007	Existem procedimentos documentados de aquisição, fabricação, montagem e testes para a parte MECÂNICA do produto ? em caso afirmativo qual o seu conteúdo ?
EMPRESA	
MRM	Sim. O conteúdo são as listas de peças e componentes de cada parte, subsistema e submontagem do produto.
008	Existem procedimentos documentados de aquisição, fabricação, montagem e testes para a parte ELETRÔNICA do produto ? em caso afirmativo qual o seu conteúdo ?
EMPRESA	

MRM	Sim. Listas detalhadas de aquisição dos componentes eletrônicos, *gerbers* para placas eletrônicas, especificações do ambiente de fabricação e montegem eletrônica, detalhamento de esquemáticos de cablagem e conexões, listas e mapas de montagem, procedimentos de montagem eletrônica, detalhamento dos procedimentos de montagem eletrônica.
009	Existem procedimentos de revisão da fabricação e montagem da parte MECÂNICA do produto?
EMPRESA	
MRM	Sim. Existem atividades de revisão da documentação Mecânica.
010	Existem procedimentos de revisão da fabricação e montagem da parte ELETRÔNICA do produto ?
EMPRESA	
MRM	Sim. Após a revisão são gerados os procedimentos detalhados de montagem eletrônica incluindo os testes a serem realizados com as partes recebidas para a montagem e os testes finais, listas e mapas de montagem eletrônica e listas de componentes eletrônicos para aquisição. Os desenhos de PCB a serem utilizados na fabricação das placas de circuito impresso devem ser detalhados.
011	Como são identificadas falhas potenciais do produto?
EMPRESA	
MRM	FMEA (*Failure Mode and Effect Analysis*).
012	Quais são os recursos necessários para produção do produto ? Esses recursos são homologados para uso em produtos de caráter cibernético?
EMPRESA	
MRM	Ex1.: Moldes de injeção plástica, estampos de corte, castanhas, grampos e dispositivos de fixação em geral, suportes de montagem, dispositivos especiais de crimpagem. Ex2.: Procedimentos de montagem eletrônica e mecânica, documentação de fabricação mecânica (folhas de processo) e eletrônica (*gerbers*) arquivos para placas de circuito.
013	Existem fornecedores para a fabricação de partes do produto (eletrônica/*software*) ? ou para manutenção e melhoria do produto ? Caso positivo, como são homologados?
EMPRESA	
MRM	As partes que compõem o produto podem ser divididas em partes fabricadas e compradas.
014	Quais atividades são realizadas para instalação e configuração de *Software* utilizado no poduto ?
EMPRESA	
MRM	Ex.: Descrição das atividades de instalação do *software*, versão válida e atividades necessárias à configuração do computador.
015	Como é avaliado a criticidade do *Software* ?
EMPRESA	
IEEE 1012	A norma define 4 níveis de integridade de *Software* para descrever sua criticidade: (4) High: A função selecionada afeta de forma crítica a performance do *software*. (3) Major: A função selecionada afeta significativamente a performance do

	software. (2) Moderate: A função selecionada afeta de forma moderada o desempenho do sistema, mas estratégias podem ser implementadas para compensar a perda de desempenho. (1) Low: A função selecionada cria inconvenientes para o usuário caso não funcione conforme os requisitos.
016	Quais as atividades realizadas para o gerenciamento da validação e verificação do *Software* ?
EMPRESA	
IEEE 1012	A norma prevê 5 tarefas mínimas para as atividades de Gerenciamento de Validação e Verificação de *Software*: (1) Plano de Verificação e Validação de *Software* (SVVP); (2) Avaliação de mudança na linha de base; (3) Gerenciamento de Revisão; (4) Gerenciamento e Suporte Técnico; (5) Interface com os Processos de suporte e organizacionais.
017	Como são realizadas as atividades para o desenvolvimento do *Software* ?
EMPRESA	
IEEE 1012	A norma prevê 5 tarefas mínimas para as atividades de Desenvolvimento do *Software*: (1) Documentação da Solução específica de Implementação para resolver o problema do usuário; (2) Definição dos Requisitos: funcionais, performance, interfaces externas para o *software*, segurança, requisitos de segurança, documentação do usuário; (3) Projeto do *Software*: Arquitetura e componentes; (4) Implementação: Codificação e Testes. Verificação e validação do *software* quanto aos itens: correção, precisão, análise crítica e de riscos; (5) Testes; (6) Instalação do *Software* no ambiente de destino.
018	Quais tipos de testes são realizados no produto ? Existem ferramentas para automação de testes do *Software* ? em caso de análise dinâmica do *Software* ?
EMPRESA	
IEEE 1012	A norma recomenda os seguintes Testes (Unidade, Integração, Sistema, Aceitação). Na análise dinâmica de testes pode-se utilizar ferramenta de automação de teste.
019	Os resultados dos testes e defeitos detectados são documentados ? Quais documentos são gerados ?
EMPRESA	
IEEE 1012	A norma recomenda a criação de documentação de Registro dos testes executados.
020	Como são analisados os impactos de mudanças no *Software*, como melhorias ou adaptações ?
EMPRESA	
IEEE 1012	A norma prevê 9 tarefas para as atividades de manutenção do *Software*:

	(1) Revisão do Plano de Verificação e Validação do *Software*; (2) Avaliação da Proposta de Mudança; (3) Avaliação de anomalias; (4) Análise de criticidade; (5) Análise de migração; (6) Análise de reestruturação; (7) Análise crítica; (8) Análise de riscos; (9) Atividades de interação.
021	As alterações no projeto são analisadas quanto ao impacto no risco de falhas do produto? E do processo? Como é avaliada ?
EMPRESA	
MRM	Sim. FMEA (*Failure mode and effect analysis*).
022	Como é realizado o controle da qualidade do processo produtivo do produto ?
EMPRESA	
MRM	Existem planos de controle para os itens críticos do processo. É realizado o detalhamento da documentação de aquisição para contribuir com o proceso de homologação dos fornecedores. É realizado a aquisição, fabricação dos moldes e dispositivos de fabricação para serem posteriormente instalados e testados.
023	Como é considerada concluída a fase de homologação do produto ?
EMPRESA	
MRM	Com a verificação da qualidade dos resultados da fase e posteriormente a documentação da mesma, gerando uma nova configuração do projeto.
024	Quais são os documentos/procedimentos que atestam que o produto foi homologado com sucesso ?
EMPRESA	
MRM	Relatório de testes de uso do protótipo de homologação, documento de posicionamento das especificações do produto, minuta do projeto e o plano de projetos.

APÊNDICE B – Formulário de análise do processo de certificação do produto

PRODUTO/SERVIÇO: <PRODUTO>	
RESPONSÁVEL:	
CARGO/FUNÇÃO:	
DATA: EMAIL:	
ITEM	**ANÁLISE DO PROCESSO DE CERTIFIÇÃO**
001	Como é feito o planejamento da certificação do produto ?
EMPRESA	
MRM	Através da análise dos resultados de testes, posicionamento das especificações do produto, refinamento da minuta do projeto quanto ao portifólio planejado, definição das marcas de qualidade certificada necessárias ao produto e planejamento dos locais e datas de certificação laboratorial e auditorias de qualidade.
002	O planejamento da certificação do produto é documentado ? qual documento ?
EMPRESA	
MRM	Sim. No plano de validação e certificação que deverá estar agregado ao plano de projetos do produto.
003	Como é feita a preparação documental do produto exigida por órgãos certificadores?
EMPRESA	
MRM	Através da documentação de uso do produto: manuais de instrução, informações gerais de segurança e relatório técnico global do produto.
004	Como é feita a comprovação de que o produto desenvolvido, fabricado e montado atende aos requisitos normativos aplicáveis ?
EMPRESA	
MRM	Através da identificação das partes do equipamento a serem substituídas, em função de eventuais alterações de projeto baseadas em requisitos normativos adicionais, necessários aos mercados nos quais o produto será introduzido. A partir deste ponto, são então fabricados e montados os subsistemas a substituir e inspeções de processo.
005	Como/Onde o produto é testado ?
EMPRESA	
MRM	São realizados testes funcionais para a verificação do produto.
006	Como é realizada a submissão do produto à certificação ?
EMPRESA	
MRM	São realizados procedimentos de testes e auditorias que permitam certificar o produto baseado em padrões internacionalmente reconhecidos. Os resultados desses testes podem demandar novas alterações no produto para adequação normativa.

APÊNDICE C – Formulário de análise baseado na Norma ISO/IEC 15408: *Common Criteria for Information Technology Security Evaluation*

PRODUTO/SERVIÇO: <PRODUTO>	
RESPONSÁVEL:	
CARGO/FUNÇÃO:	
DATA: EMAIL:	
ITEM	**ANÁLISE BASEADO NA NORMA ISO/IEC_15408**
001	A empresa identifica o Perfil de Proteção do produto com vista a certificá-lo? Como?
EMPRESA	
ISO/IEC_15408	A norma prevê a criação do documento Perfil de Proteção (PP) o qual identifica os requisitos de segurança para o produto, incluindo 6 famílias: (1) PP Introduction: Descrição do produto alvo TOE; (2) Conformance Claims: Determina a garantia da conformidade exigida; (3) Security Problem Definition: Define o problema de segurança a ser abordado pelo TOE; (4) Security Objectives: Declaração concisa da resposta ao problema de segurança; (5) Extended Components Definition: Define os requisitos de segurança extendidos; (6) Security Requirements: Define os requisitos de segurança funcional (SFRs) e requisitos de garantia de segurança (SARs).
002	Para o Desenvolvimento do Produto a empresa especifica alguns dos documentos previstos no itens abaixo ? 1. Descrição da arquitetura de segurança; 2. Especificação funcional; 3. Representação da implementação; 4. Funcionalidades de segurança interna do produto; 5. Modelo Formal da Política de Segurança; 6. Projeto do produto.
EMPRESA	
ISO/IEC_15408	A norma prevê a criação de documentos para o desenvolvimento do produto, incluindo 6 famílias: (1) Security Architecture: Descreve a arquitetura de segurança do TOE; (2) Functional specification: Descreve a especificação funcional e as interfaces de segurança do produto; (3) Implementation representation: Descreve a representação dos níveis de implementação do produto; (4) TSF internals: Aborda a avaliação da estrutura interna do TSF; (5) Security policy modelling: Fornece um modelo formal da política de segurança do TSF; (6) TOE design: Descreve o projeto do TOE.
003	A empresa fornece documentação do produto para o usuário final? Quais?

EMPRESA	
ISO/IEC_15408	A norma prevê o fornecimento de 2 documentos representados pelas famílias abaixo: (1) Operational user guidance: Guia de operação do usuário; (2) Preparative procedures: Aborda os procedimentos para que o produto seja recebido e instalado de forma segura.
004	Quais controles (documentação) são definidos durante o desenvolvimento e manutenção do produto ?
EMPRESA	
ISO/IEC_15408	A norma prevê 7 famílias para suporte ao ciclo de vida do produto descritas abaixo: (1) CM capabilities: Gerenciamento das configurações do TOE e controle dos processos; (2) CM scope: Identifica itens de configuração a serem incluídos nos requisitos do item (1); (3) Delivery: Procedimentos para a entrega segura do TOE para o usuário; (4) Development security: Descrevem itens para o desenvolvimento seguro do TOE a serem utilizados no ambiente de desenvolvimento; (5) Flaw remediation: Descrevem procedimentos para acompanhar e corrigir falhas; (6) Life-cycle definition: Define um modelo para o desenvolvimento e manutenção do TOE; (7) Tools and techniques: Seleciona as ferramentas e técnicas a serem utilizadas para o desenvovimento, análise e documentação do TOE.
005	Como é avaliada a segurança do produto ? existe documentação ?
EMPRESA	
ISO/IEC_15408	A norma prevê 7 famílias para avaliação da segurança do produto descritas abaixo: (1) ST Introduction: Descreve o TOE em 3 níveis de abstração: referência, visão geral e descrição; (2) Conformance claims: Avalia as conformidades exigidas; (3) Security problem definition: Define o problema de segurança a serem abordados para o TOE e para o ambiente operacinal; (4) Security objectives: Fornece uma declaração concisa do problema de segurança; (5) Extended components definition: Os requisitos de segurança estendidos não são baseados em componentes do (CC) Parte 2 ou Parte 3, mas são baseados em componentes definidos pelo autor do ST; (6) Security requirements: Fornecem uma declaração e justificativa dos requisitos de segurança; (7) TOE summary specification: Fornece uma visão geral de como o TOE foi implementado.
006	Quais testes são realizados no produto ?
EMPRESA	
ISO/IEC_15408	A norma descreve 4 famílias para realização dos testes do produto, que vai depender das características específicas de cada TOE: (1) Testes de cobertura (Coverage Tests): Permite testar as funcionalidades de segurança do TOE com a especificação funcional; (2) Testes de profundidade (Depth Tests): Permite realizar testes com a

	interface, componentes e módulos; (3) Testes independentes (Independent Tests): Podem incluir repetidos testes funcionais pelo desenvolvedor (incluindo partes ou "todo"), podendo estender o escopo ou a profundidade; (4) Testes funcionais (Functional Tests): Permite que o desenvolvedor realize testes funcionais.
007	Como são realizadas as análises de vulnerabilidades no produto ?
EMPRESA	
ISO/IEC_15408	A norma descreve 5 famílias para análise de possíveis vulnerabilidades introduzidas no desenvolvimento ou no (funcionamento/operacional) do produto: (1) Vulnerability Survey: Determina possíveis vulnerabilidades que podem ser facilmente encontradas por um atacante; (2) Vulnerability Analysis: É realizado testes de penetração pelo auditor considerando um ataque potencial básico; (3) Focused Vulnerability Analysis: É realizado testes de penetração pelo auditor considerando um ataque potencial do básico ao avançado; (4) Methodical Vulnerability Analysis: É realizado testes de penetração pelo auditor considerando um ataque potencial moderado; (5) Advanced Vulnerability Analysis: É realizado testes de penetração pelo auditor considerando um ataque potencial alto.
008	Como são realizadas níveis de garantia para avaliação do produto com vista a certificação ?
EMPRESA	
ISO/IEC_15408	A norma descreve 7 níveis de garantia de avaliação do produto (EAL1 a EAL7) onde cada EAL corresponde a um pacote de requisitos de garantia de segurança (SARs.) **EAL1**: Uma avaliação neste nível deverá fornecer evidências que as funções do produto são consistentes com a documentação do mesmo. Fornece um nível básico de segurança. **EAL2**: Utilizado na proteção de sistemas legados onde o acesso ao desenvolvedor pode ser limitado. Realiza análise de vulnerabilidade baseada na especificação funcional do produto alvo. Fornece um nível baixo a moderado de segurança. **EAL3**: Apresenta um aumento significativo de segurança em relação ao EAL2, por exigir uma cobertura de testes mais segura e garantir que o produto não será adulterado durante o desenvolvimento. **EAL4**: Apresenta um nível moderado a alto de segurança, além de utilizar controles no ambiente de desenvovimento, automação e procedimentos de entregas seguros. **EAL5**: Apresenta aumento significativo de segurança em relação ao EAL4 por exigir descrições do projeto semiformais e uma arquitetura mais estruturada. **EAL6**: Visa a proteção dos ativos contra riscos significativos, onde o valor dos bens protegidos justificam os custos. A análise de vulnerabilidades neste nível demonstra resistência à ataques de elevado potencial. **EAL7**: A aplicação prática deste nível é limitada aos produtos de alta segurança. Apresenta aumento significativo de segurança em relação ao EAL6, por exigir análises e testes mais abrangentes.

APÊNDICE D – Detalhamento dos requisitos de segurança do produto: baseado na Norma ISO/IEC-15408: *Common Criteria for Information Technology Security Evaluation* (CC)

O detalhamento dos requisitos de segurança aborda os seguintes objetivos:

1. Fornecer uma descrição geral dos requisitos para segurança de Produtos/Serviços de TI baseados na Norma ISO/IEC-15408: *Common Criteria for Information Technology Security Evaluation* (CC);

2. Descrever os requisitos de segurança apresentados na família: (APE_REQ) da Classe Perfil de Proteção – *Protection Profile* (PP);

3. Descrever o objetivo e algumas famílias das seguintes classes: Desenvolvimento, Documentação, Suporte ao Ciclo de Vida, Avaliação do objetivos de Segurança, Testes e Análise de Vulnerabilidades;

4. Fornecer orientações para desenvolvedores e auditores de Produtos/Serviços de TI;

5. Descrever os níveis de garantia de avaliação do produto: *Evaluation Assurance Level* (EAL1 a EAL7).

D.1 – O PERFIL DE PROTEÇÃO – PROTECTION PROFILE (PP)

Consiste em um documento criado pelo usuário ou grupo de usuários, o qual identifica os requisitos de segurança para uma classe de produtos de segurança (por exemplo, *smartcards*, *firewalls*, dentre outros.). É composto por 6 famílias: APE_INT, APE_CCL, APE_SPD, APE_ECD e 2 pacotes de avaliação padrão: APE_OBJ e APE_REQ.

Tabela 1 - Avaliação do Perfil de Proteção

CLASSE	**AVALIAÇÃO DO PERFIL DE PROTEÇÃO**
APE	**PROTECTION PROFILE EVALUATION**
Famílias	**DECOMPOSIÇÃO DA CLASSE APE**
APE_INT	PP introduction – Consultar Norma
APE_CCL	Conformance claims – Consultar Norma
APE_SPD	Security problem definition – Consultar Norma
APE_OBJ	Security objectives – Consultar Norma
APE_ECD	Extended components definition – Consultar Norma
APE_REQ	**Security requirements – Ver Tabela 2**

Fonte: Commom Criteria, 2015.

Família APE_INT - PP INTRODUCTION

O objetivo desta família é descrever o produto alvo (TOE) de forma clara. Esta descrição é necessária para que o PP seja corretamente identificado, sendo uma visão geral e consistente com as demais famílias.

Família APE_CCL - CONFORMANCE CLAIMS

O objetivo desta família é determinar a garantia da conformidade exigida. Além disso, esta família especifica como as conformidades com os *Security Target* (STs) e outros *Protection Profile* (PPs) são exigidos com o PP.

Família APE_SPD - SECURITY PROBLEM DEFINITION

O objetivo desta família é definir o problema de segurança a serem abordados pelo *Target of Evaluation* (TOE) e para o seu ambiente operacional. Além disso, é necessário demonstrar que o problema de segurança do TOE e seu ambiente operacional é claramente definido.

Família APE_OBJ - SECURITY OBJECTIVES

O objetivo desta família consite em uma declaração concisa da resposta ao problema de segurança definido na família *Security Problem Definition* (APE_SPD). A avaliação dos objetivos de segurança é necessária para demonstrar que o mesmo resolve de forma adequada o problema de definição de segurança.

Família APE_ECD – EXTENDED COMPONENTS DEFINITION

O objetivo desta família é definir os requisitos de segurança estendidos baseados em componentes definidos pelo autor do PP e que não foram claramente expressos nessa norma.

Família APE_REQ – SECURITY REQUIREMENTS

Os requisitos de segurança funcional (SFRs) estabelecem uma descrição clara do comportamento da segurança prevista para o TOE. Os requisitos de garantia de seguranca (SARs) definem as atividades esperadas que serão realizadas pelo TOE.

D.2 – FAMÍLIA: APE_REQ - REQUISITOS DE SEGURANÇA

Tabela 2 - Requisitos de Segurança Família: APE_REQ

Família	REQUISITOS DE SEGURANÇA (APE_REQ)
APE_REQ	APE_REQ.1 *Stated security requirements* Dependências : APE_ECD.1 *Extended components definition*
Elementos de Ação do Desenvolvedor:	
APE_REQ.1.1D	O desenvolvedor deverá fornecer uma declaração dos requisitos de segurança.
APE_REQ.1.2D	O desenvolvedor deverá fornecer uma justificativa para os requisitos de segurança.
Conteúdo e Elementos de Apresentação:	
APE_REQ.1.1C	A declaração de requisitos de segurança deverá descrever os requisitos funcionais de segurança (SFR) e os requisitos de garantia de segurança (SARs).
APE_REQ.1.2C	Todos os sujeitos, objetos, operações, atributos de segurança, entidades externas e outros termos que são utilizados nos (SFRs) e (SAR) deverão ser definidos.
APE_REQ.1.3C	A declaração de requisitos de segurança deverá identificar todas as operações com os mesmos.
APE_REQ.1.4C	Todas as operações devem ser executadas corretamente.
APE_REQ.1.5C	Cada dependência de requisitos de segurança deverá ser adequada ou justificada caso contrário.
APE_REQ.1.6C	A declaração dos requisitos de segurança deverá ser internamente consistente.
Elementos de Ação do Auditor:	
APE_REQ.1.1E	O Auditor deverá certificar que a informação fornecida atende a todos os requisitos do conteúdo e apresentação de evidências.
APE_REQ	**APE_REQ.2 *Derived security requirements***
Descreve os requisitos de segurança do produto que são derivados dos objetivos de segurança para o produto alvo (TOE).	
Elementos de Ação do Desenvolvedor:	
APE_REQ.2.1D	O desenvolvedor deverá fornecer uma declaração dos requisitos de segurança.
APE_REQ.2.2D	O desenvolvedor deverá fornecer uma justificativa para os requisitos de segurança.
Conteúdo e Elementos de Apresentação:	
APE_REQ.2.1C	A declaração de requisitos de segurança deverá descrever os requisitos funcionais de segurança (SFR) e os requisitos de garantia de segurança (SARs).
APE_REQ.2.2C	Todos os sujeitos, objetos, operações, atributos de segurança, entidades externas e outros termos que são utilizados nos (SFRs) e (SAR) deverão ser definidos.
APE_REQ.2.3C	A declaração dos requisitos de segurança deverá identificar todas as operações com os mesmos.
APE_REQ.2.4C	Todas as operações devem ser executadas corretamente.
APE_REQ.2.5C	Cada dependência de requisitos de segurança deverá ser adequada ou justificada caso contrário.
APE_REQ.2.6C	A justificativa dos requisitos de segurança deverá comparar cada (SFR) com os objetivos de segurança do produto alvo da avaliação (TOE).
APE_REQ.2.7C	A justificativa dos requisitos de segurança deverá demonstrar que os requisitos de segurança funcional (SFRs) cumprem todos os objetivos de segurança para o produto alvo da avaliação (TOE).
APE_REQ.2.8C	A justificativa dos requisitos de segurança deverá explicar por que os requisitos de garantia da segurança (SARs) foram escolhidos.
APE_REQ.2.9C	A declaração dos requisitos de segurança deve ser internamente consistente.
Elementos de Ação do Auditor:	
APE_REQ.2.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para conteúdo e apresentação de evidências.

Fonte: COMMON CRITERIA, 2015

D.3 – CLASSE DESENVOLVIMENTO

Os requisitos da classe desenvolvimento fornecem informações sobre o produto alvo *Target of Evaluation* (TOE). É também utilizada como base para a realização da análise de vulnerabilidades e testes do TOE. É composta por seis famílias de requisitos: ADV_ARC: *Security Architecture*, ADV_FSP: *Functional specification*, ADV_IMP: *Implementation representation*, ADV_INT: TSF *internals*, ADV_SPM: *Security policy modelling* e ADV_TDS: TOE *design*. Serão exibidos os componentes para as famílias: ADV_ARC e ADV_SPM, as demais deverão ser consultadas na norma.

Tabela 3 - Classe Desenvolvimento

CLASSE	**DESENVOLVIMENTO**
ADV	**DEVELOPMENT**
Famílias	**DECOMPOSIÇÃO DA CLASSE ADV**
ADV_ARC	**Security Architecture -** Ver Tabela 4
ADV_FSP	Functional specification – Consultar Norma
ADV_IMP	Implementation representation – Consultar Norma
ADV_INT	TSF internals – Consultar Norma
ADV_SPM	**Security policy modelling –** Ver Tabela 5
ADV_TDS	TOE design – Consultar Norma

Fonte: COMMON CRITERIA, 2015

Tabela 4 - Arquitetura de Segurança Família: ADV_ARC

Família	**ARQUITETURA DE SEGURANÇA (ADV_ARC)**
ADV_ARC	ADV_ARC.1 *Security architetture description* Dependências : ADV_FSP.1 *Basic functional specification* ADV_TDS.1 Basic design
O objetivo desta Família (ADV_ARC) é que o desenvolvedor forneça uma descrição da arquitetura de segurança da TSF. Isso permitirá que a análise das informações quando comparadas com outras evidências apresentadas pelo TSF e alcance os objetivos desejados.	
Elementos de Ação do Desenvolvedor:	
ADV_ARC.1.1D	O desenvolvedor deverá projetar e implementar o TOE para que as características de segurança da TSF sejam incluídas.
ADV_ARC.1.2D	O desenvolvedor deverá projetar e implementar a TSF para que a mesma seja capaz de proteger-se contra violação por entidades não confiáveis.
ADV_ARC.1.3D	O desenvolvedor deverá fornecer uma descrição da arquitetura de segurança do TSF.
Conteúdo e Elementos de Apresentação:	
ADV_ARC.1.1C	A descrição da arquitetura de segurança deverá estar em um nível de detalhe compatível com a descrição da aplicação dos requisitos de segurança funcional (SFR) descritos no documento de projeto do TOE.
ADV_ARC.1.2C	A descrição da arquitetura de segurança deverá descrever os domínios de segurança mantidos pela TSF de forma consistente com as SFRs.
ADV_ARC.1.3C	A descrição da arquitetura de segurança deverá descrever como o processo de inicialização do TSF é seguro.
ADV_ARC.1.3C	A descrição da arquitetura de segurança deverá demonstrar que a TSF se auto-protege contra modificações.
ADV_ARC.1.5C	A descrição da arquitetura de segurança deverá demonstrar que a TSF obsta o desvio de funcionalidade da aplicação do SFR.
Elementos de Ação do Auditor:	

ADV_ARC.1.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para conteúdo e apresentação de evidências.

Fonte: COMMON CRITERIA, 2015

Família	**MODELAGEM DA POLÍTICA DE SEGURANÇA**
ADV_SPM	Formal TOE security policy model (ADV_SPM.1)
	Dependências: ADV_FSP.4 Complete functional specification
Elementos de Ação do Desenvolvedor:	
ADV_SPM.1.1D	O desenvolvedor deverá fornecer um modelo formal da política de segurança - Modelo Formal da Política de Segurança.
ADV_SPM.1.2D	Para cada política incluída no modelo da política de segurança, deverá ser identificada as partes relevantes da comunicação de SFRs que fazem parte da mesma.
ADV_SPM.1.3D	O desenvolvedor deverá fornecer uma comprovação formal de correspondência entre o modelo e qualquer especificação funcional formal.
ADV_SPM.1.4D	O desenvolvedor deverá fornecer uma demonstração de correspondência entre o modelo e a especificação funcional.
Conteúdo e Elementos de Apresentação:	
ADV_SPM.1.1C	O modelo deverá ser um template formal, com texto explicativo e identificar as políticas de segurança do TSF que serão modeladas.
ADV_SPM.1.2C	Para todas as políticas modeladas, o modelo deverá definir a segurança para o TOE e comprovar que o mesmo não atinja um estado vulnerável.
ADV_SPM.1.3C	A correspondência entre o modelo e a especificação funcional deverá estar em um nível correto de formalidade.
ADV_SPM.1.4C	A correspondência deverá mostrar que a especificação funcional é consistente e completa em relação ao modelo.
Elementos de Ação do Auditor:	
ADV_SPM.1.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para conteúdo e apresentação de evidências.

Fonte: COMMON CRITERIA, 2015

D.4 – CLASSE DOCUMENTAÇÃO

A classe documentação fornece os requisitos de orientação ao usuário como a realização de operação segura, manipulação e configurações incorretas do TOE. É composta por duas famílias: AGD_OPE: Operational user guidance e AGD_PRE: Preparative procedures. A família AGD_OPE (Guia de operação do usuário) é destinada a todos os tipos de usuários do TOE (responsáveis pela manutenção, administração, programadores, dentre outros). Já a família AGD_PRE apresenta procedimentos para garantir que o TOE seja recebido e instalado de forma segura como esperado pelo desenvolvedor.

Tabela 5 - Classe Documentação

CLASSE	**GUIA DE DOCUMENTAÇÃO**
AGD	**GUIDANCE DOCUMENTS**
Famílias	**DECOMPOSIÇÃO DA CLASSE AGD**
AGD_OPE	Operational user guidance – Ver Tabela 7
AGD_PRE	Preparative procedures – Ver Tabela 7

Fonte: COMMON CRITERIA, 2015

Tabela 6 - Guia de operação do usuário famílias: AGD:OPE e AGD_PRE

Família	**GUIA DE OPERAÇÃO DO USUÁRIO**
AGD_OPE	AGD_OPE.1 *Operational user guidance* Dependências : ADV_FSP.1 *Basic functional specification*
	A única documentação necessária é uma especificação de todos TSFIs e uma descrição em alto nível de aplicação do SFR que sirva como suporte ao SFR TSFIs. Para garantir que os aspectos "importantes" da TSF foram definidos corretamente no TSFIs. O desenvolvedor é obrigado a fornecer o objetivo e o método de utilização, parâmetros para o cumprimento do SFR e com suporte ao TSFIs e SFR.
Elementos de Ação do Desenvolvedor:	
AGD_OPE.1.1D	O desenvolvedor deverá fornecer um guia de operação do usuário. Que deverá conter os itens abaixo:
Conteúdo e Elementos de Apresentação:	
AGD_OPE.1.1C	O guia deverá descrever para cada função do usuário as funções e privilégios acessíveis ao mesmo que devem ser controladas em um ambiente de processamento seguro. Incluindo advertências adequadas.
AGD_OPE.1.2C	O guia deverá descrever para cada função do usuário como utilizar as interfaces disponíveis fornecidas pelo produto alvo da avalação (TOE) de forma segura.
AGD_OPE.1.3C	O guia deverá descrever para cada função do usuário as funções e interfaces disponíveis, incluindo todos os parâmetros de segurança indicando os valores seguros como apropriados.
AGD_OPE.1.4C	O guia deverá descrever para cada função do usuário cada tipo de evento relevante de segurança em relação às funções de acesso do usuário que precisam ser executadas. Incluindo mudanças das características de segurança de controle da TSF.
AGD_OPE.1.5C	O guia deverá identificar todas as formas possíveis de operação do TOE (incluindo operações de falha ou erro operacional) suas consequências e implicações para manutenção segura.
AGD_OPE.1.6C	O guia deverá descrever medidas de segurança a serem seguidas com o intuito de cumprir os objetivos de segurança para o ambiente operacional, como descrito no ST.
AGD_OPE.1.7C	O guia deverá ser claro.
Elementos de Ação do Auditor:	
AGD_OPE.1.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.
Família	**PREPARAÇÃO DOS PROCEDIMENTOS**
AGD_PRE	AGD_OPE.1 *Operational user guidance*
	Aborda procedimentos para que o produto seja recebido e instalado de forma segura.
Elementos de Ação do Desenvolvedor:	
AGD_PRE.1.1D	O desenvolvedor deverá fornecer o TOE incluindo seus procedimentos.
Conteúdo e Elementos de Apresentação:	
AGD_PRE.1.1C	Os procedimentos de preparação deverão descrever todas as medidas necessárias para aceitação segura das entregas conforme os procedimentos de entrega do desenvolvedor.
AGD_PRE.1.2C	Os procedimentos de preparação deverão descrever todas as medidas necessárias para instalação segura do TOE e para a preparação segura do ambiente operacional em conformidade com os objetivos de segurança descritos na ST.
Elementos de Ação do Auditor:	
AGD_PRE.1.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.
AGD_PRE.1.2E	O Auditor deverá aplicar os procedimentos de preparação para confirmar que o TOE pode ser concebido de forma segura para seu funcionamento.

Fonte: COMMON CRITERIA, 2015

D.5 – CLASSE SUPORTE AO CICLO DE VIDA

A classe suporte ao ciclo de vida estabelece um controle nos processos do TOE durante o desenvolvimento e manutenção. No ciclo de vida do produto o TOE é separado em dois tipos: ou está sobre a responsabilidade do desenvolvedor (TOE no desenvolvimento) ou sobre a responsabilidade do usuário (TOE no ambiente do usuário). O ponto de transição é exatamente onde o TOE é entregue ao usuário. Este é também considerado o ponto de transição da classe Suporte ao Ciclo de Vida (ALC) à classe Documentação (AGD). É composta por sete famílias: ALC_CMC: CM *capabilities*, ALC_CMS: CM *scope*, ALC_DEL: *Delivery*, ALC_DVS: *Development security*, ALC_FLR: *Flaw remediation*, ALC_LCD: *Life-cycle definition* e ALC_TAT: *Tools and techniques*. Serão exibidos os componentes para a família ALC_DVS (*Development security*), as demais deverão ser consultadas na norma

Tabela 7 - Classe suporte ao ciclo de vida

CLASSE	**SUPORTE AO CICLO DE VIDA**
ALC	**LIFE-CYCLE SUPPORT**
Famílias	**DECOMPOSIÇÃO DA CLASSE ALC**
ALC_CMC	CM capabilities – Consultar Norma
ALC_CMS	CM scope – Consultar Norma
ALC_DEL	Delivery – Consultar Norma
ALC_DVS	**Development security – Ver Tabela 9**
ALC_FLR	Flaw remediation – Consultar Norma
ALC_LCD	Life-cycle definition – Consultar Norma
ALC_TAT	Tools and techniques – Consultar Norma

Fonte: COMMON CRITERIA, 2015

Tabela 8 - Desenvolvimento seguro família: ALC_DVS

Família	**DESENVOLVIMENTO SEGURO**
ALC_DVS	ALC_DVS.1 *Identification of security measures* Dependências : Não há.
Elementos de Ação do Desenvolvedor:	
ALC_DVS.1.1D	O desenvolvedor deverá produzir e fornecer uma documentação para desenvolvimento seguro.
Conteúdo e Elementos de Apresentação:	
ALC_DVS.1.1C	A documentação para desenvolvimento seguro deverá descrever o material, procedimentos, pessoas e outras medidas de segurança necessárias para proteção da confidencialidade e integridade do projeto do TOE e seu ambiente de desenvolvimento.
Elementos de Ação do Auditor:	
ALC_DVS.1.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.
ALC_DVS.1.2E	O Auditor deverá confirmar que as medidas de segurança são aplicadas.

Fonte: COMMON CRITERIA, 2015

Tabela 9 - Desenvolvimento seguro família: ALC_DVS

ALC_DVS	ALC_DVS.2 *Sufficiency of security measures* Dependências : Não há.
Elementos de Ação do Desenvolvedor:	
ALC_DVS.2.1D	O desenvolvedor deverá produzir e fornecer uma documentação para desenvolvimento seguro.
Conteúdo e Elementos de Apresentação:	
ALC_DVS.2.1C	A documentação para desenvolvimento seguro deverá descrever o material, procedimentos, pessoas e outras medidas de segurança necessárias para proteção da confidencialidade e integridade do projeto do TOE e seu ambiente de desenvolvimento.
ALC_DVS.2.2C	A documentação para desenvolvimento seguro deverá justificar que as medidas de segurança fornecem o nível de protecção necessário para manter a confidencialidade e integridade do TOE.
Elementos de Ação do Auditor:	
ASE_DVS.2.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.
ASE_DVS.2.2E	O Auditor deverá confirmar que as medidas de segurança são aplicadas.

Fonte: COMMON CRITERIA, 2015

D.6 – CLASSE AVALIAÇÃO DO OBJETIVO DE SEGURANÇA

A classe Avaliação de um *Security Target* (ST) é necessária para demonstrar que o produto é resistente internamente, assim como identificar se o mesmo é baseado em um ou mais *Protection Profile* (PP) e pacotes. Essas propriedades são necessárias para que o (ST) seja adequado para utilização como base de avaliação do TOE. É composta por sete famílias: ASE_INT: ST *Introduction*, ASE_CCL: *Conformance claims*, ASE_SPD: *Security problem definition*, ASE_OBJ: *Security objectives*, ASE_ECD: *Extended components definition*, ASE_REQ: *Security requirements*, ASE_TSS: TOE *summary specification*. Serão exibidos os componentes para a família ASE_REQ (*Security requirements*), as demais deverão ser consultadas na norma.

Tabela 10 - Classe avaliação do objetivo de segurança

CLASSE	**AVALIAÇÃO DO OBJETIVO DE SEGURANÇA**
ASE	**SECURITY TARGET EVALUATION**
Famílias	**DECOMPOSIÇÃO DA CLASSE ASE**
ASE_INT	ST Introduction – Consultar Norma
ASE_CCL	Conformance claims – Consultar Norma
ASE_SPD	Security problem definition – Consultar Norma
ASE_OBJ	Security objectives – Consultar Norma
ASE_ECD	Extended components definition – Consultar Norma
ASE_REQ	**Security requirements – Ver Tabela 11**
ASE_TSS	TOE summary specification – Consultar Norma

Fonte: COMMON CRITERIA, 2015

Tabela 11 - Requisitos de segurança família: ASE_REQ

Família	REQUISITOS DE SEGURANÇA
ASE_REQ	ASE_REQ.1 *Stated security requirements* Dependências : ASE_ECD.1 *Extended components definition*
Elementos de Ação do Desenvolvedor:	
ASE_REQ.1.1D	O desenvolvedor deverá fornecer uma declaração dos requisitos de segurança.
ASE_REQ.1.2D	O desenvolvedor deverá fornecer uma justificativa para os requisitos de segurança.
Conteúdo e Elementos de Apresentação:	
ASE_REQ.1.1C	A declaração dos requisitos de segurança deverá relatar os requisitos funcionais de segurança (SFR) e os requisitos de garantia de segurança (SARs).
ASE_REQ.1.2C	Todos os sujeitos, objetos, operações, atributos de segurança, entidades externas e outros termos que são utilizados nos SFRs e nos SAR deverão ser definidos.
ASE_REQ.1.3C	A declaração dos requisitos de segurança deverá identificar todas as operações com os mesmos.
ASE_REQ.1.4C	Todas as operações devem ser executadas corretamente.
ASE_REQ.1.5C	Cada dependência dos requisitos de segurança deverá ser adequada ou ser justificada caso contrário.
ASE_REQ.1.6C	A declaração dos requisitos de segurança deverá ser internamente consistente.
Elementos de Ação do Auditor:	
ASE_REQ.1.1E	O Auditor deverá certificar que a informação fornecida atende a todos os requisitos do conteúdo e apresentação de evidências.
ASE_REQ	ASE_REQ.2 *Derived security requirements* Dependências : ASE_OBJ.2 *Security objectives* ASE_ECD.1 *Extended components definition*
Elementos de Ação do Desenvolvedor:	
ASE_REQ.2.1D	O desenvolvedor deverá fornecer uma declaração dos requisitos de segurança.
ASE_REQ.2.2D	O desenvolvedor deverá fornecer uma justificativa para os requisitos de segurança.
Conteúdo e Elementos de Apresentação:	
ASE_REQ.2.1C	A declaração dos requisitos de segurança deverá relatar os requisitos funcionais de segurança (SFR) e os requisitos de garantia de segurança (SARs).
ASE_REQ.2.2C	Todos os sujeitos, objetos, operações, atributos de segurança, entidades externas e outros termos que são utilizados nos SFRs e nos SAR deverão ser definidos.
ASE_REQ.2.3C	A declaração dos requisitos de segurança deverá identificar todas as operações com os mesmos.
ASE_REQ.2.4C	Todas as operações devem ser executadas corretamente.
ASE_REQ.2.5C	Cada dependência dos requisitos de segurança deverá ser adequada ou ser justificada caso contrário.
ASE_REQ.2.6C	A análise dos requisitos de segurança deverá comparar cada SFR com os objetivos de segurança do TOE.
ASE_REQ.2.7C	A análise dos requisitos de segurança deverá demonstrar que os SFRs cumprem todos os objetivos de segurança para o TOE.
ASE_REQ.2.8C	A análise dos requisitos de segurança deverá justificar por que os SARs foram escolhidos.
ASE_REQ.2.9C	A declaração dos requisitos de segurança deverá ser internamente consistente.
Elementos de Ação do Auditor:	
ASE_REQ.2.1E	O Auditor deverá certificar que a informação fornecida atende a todos os requisitos do conteúdo e apresentação de evidências.

Fonte: COMMON CRITERIA, 2015

D.7 – CLASSE TESTES

A Classe testes tem como objetivo confirmar que a TSF opera em conformidade com as especificações de projeto do TOE. É composta por quatro famílias: ATE_COV: Testes de Cobertura, ATE_DPT: Testes de Profundidade, ATE_IND: Testes Independentes e ATE_FUN: Testes funcionais. Serão exibidos os componentes para a família ATE_COV (Testes de Cobertura), as demais deverão ser consultadas na norma.

Tabela 12 - Classe testes

CLASSE	**AVALIAÇÃO DOS TESTES**
ATE	**TESTS**
Objetivo:	O objetivo desta classe é a confirmação que a TSF opera conforme especificações do projeto. Esta classe não aborda testes de penetração, que são baseados na análise da TSF que visa especificamente a identificação de vulnerabilidades na criação e implementação da TSF. Testes de Penetração são tratados separadamente como um aspecto da avaliação de vulnerabilidades na Classe de avaliação de vulnerabilidade (AVA).
Famílias	**DECOMPOSIÇÃO DA CLASSE ATE**
ATE_COV	**Testes de Cobertura (Coverage) – Ver Tabela 13**
ATE_COV.3	**Rigorous Analysis of Coverage – Ver Tabela 13**
ATE_DPT	Testes de Profundidade (Depth) – Consultar Norma
ATE_FUN	Testes Funcionais (Functional Tests) – Consultar Norma
ATE_IND	Testes Independenes (Independent Testing) – Consultar Norma

Fonte: COMMON CRITERIA, 2015

Tabela 13 - Testes de cobertura família: ATE_COV

Família	**ANÁLISE RÍGIDA DE COBERTURA**
ATE_COV.3	Dependências : ADV_FSP.2 Security-enforcing functional specification ATE_FUN.1 Functional testing
Objetivo	O objetivo dessa família é confirmar que o desenvolvedor realizou testes exaustivos de todas as interfaces da especificação funcional. Busca certificar que todos os parâmetros do (TSFIs) foram testados.
Elementos de Ação do Desenvolvedor:	
ATE_COV.3.1D	O desenvolvedor deverá fornecer uma análise da cobertura do teste.
Conteúdo e Elementos de Apresentação:	
ATE_COV.3.1C	A análise da cobertura dos testes deverá demonstrar a relação entre os testes da documentação de testes e os (TSFIs) da especificação funcional.
ATE_COV.3.2C	A análise da cobertura de testes deverá demonstrar que todos (TSFIs) da especificação funcional foram completamente testados.
Elementos de Ação do Auditor:	
ATE_COV.3.1D	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.

Fonte: COMMON CRITERIA, 2015

D.8 – CLASSE ANÁLISE DE VULNERABILIDADES

A Classe Análise de Vulnerabilidades explora possíveis vulnerabilidades introduzidas no desenvolvimento ou no (funcionamento/operacional) do TOE. Vulnerabilidades de desenvolvimento podem ocorrer devido alguma propriedade do TOE introduzida durante o seu desenvolvimento, como por exemplo a tentativa de adulterar a proteção de funcionalidades de segurança do mesmo. Por outro lado, vulnerabilidades operacionais levam vantagens das fraquezas dos procedimentos de contramedidas de segurança como por exemplo uma configuração incorreta. É composta por cinco famílias: AVA_VAN.1: Vulnerability Survey, AVA_VAN.2: Vulnerability Analysis, AVA_VAN.3: Focused Vulnerability Analysis, AVA_VAN.4: Methodical Vulnerability Analysis e AVA_VAN.5: Advanced Methodical Vulnerability Analysis. Serão exibidos os componentes para a família AVA_VAN.2 (Vulnerability Analysis), as demais deverão ser consultadas na norma.

Tabela 14 - Classe análise de vulnerabilidades

CLASSE	**ANÁLISE DE VULNERABILIDADES**
AVA	**VULNERABILITY ASSESSMENT**
Objetivo:	A análise de vulnerabilidades é uma avaliação para determinar se o potencial da vulnerabilidade identificada, durante a avaliação do desenvolvimento e funcionamento esperado do TOE ou por outros métodos (ex.: falhas de hipóteses ou análise quantitativa ou estatística do comportamento dos mecanismos de segurança básicos), permitem que invasores violem os requisitos de segurança funcional (SFRs).
Famílias	**DECOMPOSIÇÃO DA CLASSE AVA**
AVA_VAN.1	Vulnerability Survey – Consultar Norma
AVA_VAN.2	**Vulnerability Analysis – Ver Tabela 15**
AVA_VAN.3	Focused Vulnerability Analysis – Consultar Norma
AVA_VAN.4	Methodical Vulnerability Analysis – Consultar Norma
AVA_VAN.5	Advanced Methodical Vulnerability Analysis – Consultar Norma

Fonte: COMMON CRITERIA, 2015

Tabela 15 - Análise de vulnerabilidades família: AVA_VAN.2

Família	ANÁLISE DE VULNERABILIDADES
AVA_VAN.2	Dependências : ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design, AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Objetivo	A análise de vulnerabilidades é realizada pelo auditor para determinar a presença de possíveis vulnerabilidades. O auditor realiza testes de penetração, considerando um ataque potencial ou básico, para confirmar que as possíveis vulnerabilidades não são exploradas no ambiente operacional para o TOE.
Elementos de Ação do Desenvolvedor:	
AVA_VAN.2.1D	O desenvolvedor deverá fornecer o TOE para testes.
Conteúdo e Elementos de Apresentação:	
AVA_VAN.2.1C	O TOE deverá ser adequado para o teste.
Elementos de Ação do Auditor:	
AVA_VAN.2.1E	O Auditor deverá confirmar que a informação fornecida atende a todos os requisitos para a capacidade e apresentação de evidências.
AVA_VAN.2.2E	O auditor deverá realizar uma busca de fontes de domínio público para identificar potenciais vulnerabilidades no TOE.
AVA_VAN.2.3E	O auditor deverá realizar uma análise de vulnerabilidades independente do TOE utilizando o guia da documentação, especificação funcional, projeto do TOE e descrição da arquitetura de segurança para identificar potenciais vulnerabilidades no TOE.
AVA_VAN.2.4E	O auditor deverá realizar testes de penetração, com base na identificação de vulnerabilidades potenciais, para determinar se o TOE é resistente a ataques realizados por um atacante que possua potencial de ataque básico.

Fonte: COMMON CRITERIA, 2015

D.9 – NÍVEIS DE GARANTIA DE AVALIAÇÃO DO PRODUTO

Os níveis de garantia de avaliação do produto (EAL1 a EAL7) descrevem a profundidade com que a avaliação é realizada. Cada EAL corresponde a um pacote de requisitos de garantia da segurança (SARs), o qual cobre o desenvolvimento completo de um produto com um determinado nível de exatidão. As características do produto avaliado que foram definidas conforme o documento do alvo de segurança (ST) que descreve os requisitos de segurança funcional (SFRs) do produto servirão de base para a escolha de um dos níveis (EAL1 a EAL7).

EALs mais elevados não necessariamente representam uma “melhor segurança”, significam apenas que o nível de segurança foi testado de maneira mais extensiva. Os níveis de garantia descritos na norma ISO/IEC-15408 apresenta um determinado conjunto de funcionalidades de segurança, mas não é suficiente para garantir que este seja seguro

apenas por seguir esse padrão. A segurança do produto está relacionada à sua capacidade de resistir à ataques, sendo necessário uma avaliação completa do ambiente e das interfaces de comunicação nas quais o produto encontra-se inserido.

D.10 – EAL1 - *Functionally tested*

Fornece uma avaliação do produto alvo conforme disponibilizado para o cliente, incluindo testes independentes e orientações na documentação. Uma avaliação neste nível deverá fornecer evidências que as funções do produto são consistentes com a documentação do mesmo. Fornece um nível básico de segurança.

Figura 1 - EAL1 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Fonte: COMMON CRITERIA, 2015

D.11 – EAL2 - *Structurally tested*

Solicita a cooperação do desenvolvedor em relação ao fornecimento de informações do projeto e resultados dos testes. Este nível não implica em aumento de custo e tempo e apresenta nível baixo a moderado de segurança. Utilizado na proteção de sistemas legados onde o acesso ao desenvolvedor pode ser limitado. Realiza análise de vulnerabilidade baseada na especificação funcional do produto alvo.

Figura 2 - EAL2 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Fonte: COMMON CRITERIA, 2015

D.12 – EAL3 - *Methodically tested and checked*

É aplicável em situações onde o desenvolvedor/usuário necessita de um nível moderado de segurança e profunda investigação do produto alvo. Incluem testes, análise de vulnerabilidades, controles do ambiente e procedimentos de entregas seguros. Apresenta um aumento significativo de segurança em relação ao EAL2, por exigir uma cobertura de testes mais segura e garantir que o produto não será adulterado durante o desenvolvimento.

Figura 3 – EAL3 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Fonte: COMMON CRITERIA, 2015

D.13 – EAL4 - *Methodically designed, tested, and reviewed*

Permite que o desenvolvedor obtenha garantia máxima de segurança baseado em boas práticas de desenvolvimento comercial. Apresenta um nível moderado a alto de segurança, além de utilizar controles no ambiente de desenvovimento, automação e procedimentos de entregas seguros.

Figura 4 - EAL4 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Fonte: COMMON CRITERIA, 2015

D.14 – EAL5 – *Semiformally designed and tested*

Permite obter uma garantia máxima em segurança baseada em práticas rigorosas de desenvolvimento comercial. Neste nível os custos adicionais relativos ao desenvolvimento sem a aplicação de técnicas especializadas não será alto. Apresenta aumento significativo de segurança em relação ao EAL4 por exigir descrições do projeto semiformais e uma arquitetura mais estruturada.

Figura 5 – EAL5 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Semiformal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4 Methodical vulnerability analysis

Fonte: COMMON CRITERIA, 2015

D.15 – EAL6 – *Semiformally verified design and tested*

Permite elevada garantia da segurança e provê um ambiente de desenvolvimento rigoroso para o produto alvo. Visa a proteção dos ativos contra riscos significativos, onde o valor dos bens protegidos justificam os custos. A análise de vulnerabilidades neste nível demonstra resistência à ataques de elevado potencial.

Figura 6 – EAL6 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.5 Complete semiformal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Fonte: COMMON CRITERIA, 2015

D.16 – EAL7 – *Formally verified design and tested*

Aplicável ao desenvolvimento seguro do produto alvo em situações de risco extremo ou o valor dos ativos justificam os custos elevados. A aplicação prática deste nível é limitada aos produtos de alta segurança. Apresenta aumento significativo de segurança em relação ao EAL6, por exigir análises e testes mais abrangentes.

Figura 7 – EAL7 – Classes e componentes de garantia

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.4 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Fonte: COMMON CRITERIA, 2015